ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА»

В.М. ЧЕРНОВ, А.О.КОРЕПАНОВ

ТЕОРЕТИКО-ЧИСЛОВЫЕ ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Утверждено Редакционно-издательским советом университета в качестве учебного пособия

САМАРА
Издательство СГАУ
2006

УДК 519.2
ББК 22.343
Ч493

Инновационная образовательная программа "Развитие центра компетенции и подготовка специалистов мирового уровня в области аэрокосмических и геоинформационных технологий"

Рецензенты: д-р. техн. наук, проф. В.Г. Карташевский,
д-р. физ.-мат. наук, проф. А.И. Жданов.

Чернов В.М.

Ч493 **Теоретико-числовые преобразования в задачах цифровой обработки сигналов**: учеб. пособие / *В.М. Чернов, А.О. Корепанов* – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2006. – 112 с.

ISBN 5-7883-0398-2

Содержание пособия относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел).

Специалисты в области анализа и обработки цифровой информации давно и успешно используют алгебраические и теоретико-числовые методы, прежде всего в таких областях, как криптография, корректирующие коды, синтез быстрых алгоритмов дискретных ортогональных преобразований. Несмотря на это, существует относительно мало доступной монографической литературы, охватывающей не только одну или несколько из указанных уже традиционных областей применения методов абстрактной алгебры и теории чисел к решению задач информатики, но и рассматривающей относительно новые приложения указанных математических методов и теорий к решению перспективных задач анализа цифровых сигналов. Ряд монографий отечественных или зарубежных авторов давно уже стал библиографической редкостью, а книги, изданные за рубежом, практически недоступны широкому кругу специалистов. Данное пособие ставит своей целью частичное восполнение указанного пробела.

Предназначено для студентов специальностей и направлений «Прикладные математика и физика», «Прикладные математика и информатика».

УДК 519.2
ББК 22.343

ISBN 5-7883-0398-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

При вычислении свертки двух N-периодических последовательностей спектральным методом с помощью теоремы о свертке (см., например, [1], [2]) и использовании дискретного преобразования Фурье значения сворачиваемых последовательностей считаются, как правило, принадлежащими полю рациональных чисел $\mathbf{Q}$ (естественное "пользовательское" допущение) или, после соответствующего масштабирования, принадлежащими кольцу целых чисел $\mathbf{Z}$. В то же время значения базисных функций дискретного преобразования Фурье принадлежит полю комплексных чисел $\mathbf{C}$ - алгебраическому расширению $\mathbf{R}(i)$ поля $\mathbf{R}$ с индуцированной метрикой, связанной с обычным понятием модуля комплексного числа, которое, в свою очередь, является пополнением поля $\mathbf{Q}$ относительно метрики, связанной с абсолютной величиной числа. Таким образом, поле $\mathbf{Q}$ вкладывается в полное поле $\mathbf{C}$, причем при реализации на ЭВМ в силу конечноразрядного представления чисел вычисление преобразования (1.2) производится в $\mathbf{Q}(i)$, что приводит к погрешности, часто весьма значительной.

Для ряда задач цифровой обработки сигналов (задач криптографии, задачи умножения больших целых чисел, в частности) *принципиально* не допускается "приближенный" ответ. Либо точный, либо – не ответ. Паллиативным решением в этом случае является использование вместо дискретного преобразования Фурье его "модулярных аналогов" – теоретико-числовых преобразований (ТЧП, преобразований Фурье-Галуа).

Модулярные вычисления можно интерпретировать как "приближенные вычисления" в некоторой алгебраической структуре,

причем эта "приближенность" характеризуется делимостью "погрешности" на простое число p.

Одной из целей данного пособия является метрическая формализация вышеприведенной интерпретации, что позволило бы с единой точки зрения проанализировать, как и особенности спектральных методов вычисления свертки, так и экстраполировать эти спектральные методы для вложений поля $\mathbf{Q}$ в его пополнения относительно других, так называемых неархимедовых, метрик поля $\mathbf{Q}$. Реализация программы для тех или иных конкретных метрик позволит с единой точки зрения анализировать точность как известных алгоритмов (ДПФ, преобразование Фурье-Галуа), так и позволит увеличить точность вычисления свертки даже при относительно скромных вычислительных возможностях.

ЧАСТЬ 1. МОДУЛЯРНАЯ АРИФМЕТИКА И БЫСТРОЕ "БЕЗОШИБОЧНОЕ" ВЫЧИСЛЕНИЕ СВЕРТКИ

Реальный мир полон отвратительных чисел типа 0,79134989…, мир же компьютеров имеет дело с милыми числами типа 0 и 1.

Дж.Конвей, Н.Слоэн[1].

1.1. Постановка задачи, основные идеи

1.1.1. Теоретико-числовые преобразования и целочисленные свертки

При вычислении свертки двух N-периодических последовательностей

$$(x * y)(k) = z(k) = \sum_{n=0}^{N-1} x(n)\, y(k-n), \quad k = 0,\ldots,N-1 \qquad (1.1)$$

спектральным методом с помощью теоремы о свертке (см., например, [1], [2])

$$\hat{z}(m) = \hat{x}(m)\,\hat{y}(m),\ m = 0,\ldots,N-1,$$

$$z(k) = \frac{1}{N}\sum_{m=0}^{N-1} \hat{z}(m) h_{-m}(k),\ k = 0,\ldots,N-1,$$

где

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\ \ h_m(n),\ m = 0,\ldots,N-1, \qquad (1.2)$$

---

[1] Дж.Конвей, Н.Слоэн. *Упаковки шаров, решетки и группы*. М.:Мир, 1990.

$$h_m(n) = \exp\left\{2\pi i \frac{mn}{N}\right\}$$

есть дискретное преобразование Фурье (ДПФ), а

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} \hat{x}(m) h_{-m}(n), n = 0,\ldots,N-1$$

- обратное дискретное преобразование Фурье (ОДПФ), значения последовательностей $x(n)$ и $y(n)$ считаются, как правило, принадлежащими полю рациональных чисел **Q** (естественное "пользовательское" допущение) или, после соответствующего масштабирования, принадлежащими кольцу целых чисел **Z**. В то же время значения базисных функций $h_m(n)$ дискретного преобразования Фурье принадлежит полю комплексных чисел **C** - алгебраическому расширению **R**(i) поля **R** с индуцированной метрикой, связанной с обычным понятием модуля комплексного числа, которое, в свою очередь, является пополнением поля **Q** относительно метрики, связанной с абсолютной величиной числа. Таким образом, поле **Q** вкладывается в полное поле **C**, причем при реализации на ЭВМ в силу конечноразрядного представления чисел вычисление преобразования (1.2) производится в **Q**(i), что приводит к погрешности, часто весьма значительной.

Для ряда задач цифровой обработки сигналов (задач криптографии, задачи умножения больших целых чисел, в частности) *принципиально* не допускается "приближенный" ответ. Либо точный, либо – не ответ. Паллиативным решением в этом случае является использование вместо дискретного преобразования Фурье (1.2.) его "модулярных аналогов" – теоретико-числовых преобразований (ТЧП, преобразований Фурье-Галуа):

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\omega^{mn} \pmod{p},\ \omega^N \equiv 1 \pmod{p}. \qquad (1.3)$$

Теорема о свертке остается справедливой и в этом случае, но уже для свертки (1.1), понимаемой не в целочисленной арифметике

кольца **Z**, а в арифметике конечного поля $(\mathrm{mod}\ p)$, существенно отличающейся от арифметики кольца **Z**.

Основная идея. ***Давайте выберем простое число p достаточно большим, а именно:***

$$p > \max_{0\le n<N}\{x(n)\}\max_{0\le n<N}\{h(n)\}N,\ 0 < x(n), h(n) \in \mathbf{Z}. \qquad (1.4)$$

Тогда наименьший неотрицательный вычет значения целочисленной свертки, вычисляемой непосредственно по формуле (1.1), равен значению этой свертки. При вычислении свертки (1.1) с помощью теоретико-числовых преобразований результаты промежуточных вычислений могут превзойти число p и полученные значения компонент свертки оказываются "вычисленными с ошибкой", а именно, с точностью до слагаемого, делящегося на **число** ***p. Выбор числа p с условием (1.4) в сочетании с (грубой) априорной информацией о диапазоне изменения значений сворачиваемых функций позволяет утверждать, что найденные значения свертки являются точными (следующее целое число, отличающееся от найденного слагаемым, делящимся на p , "слишком велико").***

Таким образом, модулярные вычисления можно интерпретировать как "приближенные вычисления" в некоторой алгебраической структуре, причем эта "приближенность" характеризуется делимостью "погрешности" на простое число *p*.

Отметим, что вычисление свертки (1.1) с помощью ТЧП содержит ряд вполне объективных трудностей, связанных с арифметическими особенностями конечных полей:

- арифметические операции $(\mathrm{mod}\ p)$ не являются "элементарными компьютерными операциями", а простые числа p с "дружественными" для машинной реализации свойствами модулярных операций встречаются в натуральном ряду достаточно редко;

• в отличие от поля комплексных чисел, в конечном поле **GF**(*p*) (поле классов вычетов по простому $(\mathrm{mod}\ p)$) существуют корни не любой степени N единицы, а только удовлетворяющие условию делимости $N \mid (p\text{-}1)$.

К сожалению, эти особенности отчасти конфликтуют между собой: "хорошие" для машинной реализации операций простые числа имеют "плохие" делители числа $(p-1)$, что несколько осложняет алгоритмическую поддержку вычислений ТЧП и наоборот. Поэтому актуальной задачей задачей является разработка компромиссных решений, базирующихся на использовании представления элементов конечных полей в специальных системах счисления.

1.2. Реализация арифметических операций для модулей специального вида

Настоящий раздел имеет вспомогательный характер и включен лишь для удобства цитирования. По крайней мере, по теме двух его первых подразделов существует множество публикаций, в которых рассматриваются различные версии программной и аппаратной реализации арифметических операций в кольцах классов вычетов по модулям простых чисел специального вида – простых чисел Мерсенна и Ферма. Краткий анализ этих работ приведен в заключительных комментариях. Несколько меньшей известностью пользуются простые числа Голомба (раздел 1.2.3) и их мы рассматриваем чуть более подробно также в разделе 1.3.1.

1.2.1. Арифметика в полях по модулю числа Мерсенна

Простым числом Мерсенна называется простое число вида $p = 2^q - 1$. Из вида числа Мерсенна сразу следует необходимое (но не достаточное) ограничение на число q, которое также должно быть простым.

Сформулируем основные правила вычислений в поле $\mathbf{M} \cong \mathbf{Z}/p\mathbf{Z}$, $p = 2^q - 1$:

1) любой элемент поля $\mathbf{M}$ *представляется в форме*

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{q-1} 2^{q-1}, \quad x_j \in \{0,1\}; \qquad (1.5)$$

2) это представление однозначно для всех $0 \neq x \in \mathbf{M}$*; нулевой элемент представим двумя способами в форме* (1.5)*:*

$$0 \cdot 2^0 + \ldots + 0 \cdot 2^{q-1} \equiv 1 \cdot 2^0 + \ldots + 1 \cdot 2^{q-1} \equiv 2^q - 1 \equiv 0 \pmod{p};$$

3) так как $2^q \equiv 1 \pmod{p}$*, то в случае возникновения "бита переполнения"* $1 \cdot 2^q$ *при вычислениях эта единица "самого старшего разряда" переносится в "самый младший разряд" и суммируется с полученным числом;*

4) умножение элемента $x \in \mathbf{M}$ *на элемент* $2 \in \mathbf{M}$ *равносильно циклическому сдвигу "цифр"* x_j *в представлении* (1.5)*:*

$$2x = x_{q-1} 2^0 + x_0 2^1 + \ldots + x_{q-2} 2^{q-1};$$

5) умножение элементов поля $\mathbf{M}$ *"столбиком" сводится к циклическим перестановкам цифр и сложениям;*

6) мультипликативный порядок элемента $2 \in \mathbf{M}$ *равен* q*:* $\mathbf{Ord}(2) = q$ *(следовательно, при* $\omega = 2 \in \mathbf{M}$ *возможна реализация ТЧП* (1.3) *длины* $N = q$ *без умножений);*

7) мультипликативный порядок элемента $(-2) \in \mathbf{M}$ *равен* $2q$*:* $\mathbf{Ord}(-2) = 2q$ *(следовательно, при* $\omega = (-2) \in \mathbf{M}$ *возможна реализация ТЧП* (1.3) *длины* $N = 2q$ *без умножений);*

8) максимальная степень двойки, делящая число $(p-1)$*, равна единице.*

Следует заметить, что свойства 1-5, сформулированные выше, остаются справедливыми и для составных чисел Мерсенна. Отметим также, что последнее свойство чисел Мерсенна несколько осложняет задачу эффективного вычисления ТЧП Мерсенна, так как

требование делимости $N|(p-1)$ приводит к необходимости синтеза быстрых алгоритмов таких преобразований для весьма "экзотических" длин N. Например,

$$\left(2^{31}-1\right)-1=2\cdot\left(2^{30}-1\right)=2\cdot 3^2\cdot 7\cdot 11\cdot 31\cdot 151\cdot 331$$

и так далее.

Паллиативным способом преодоления указанной трудности является рассмотрение ТЧП в "комплексном поле Мерсенна"

$$\mathbf{M}(i)=\left\{z: a+bi;\ a,b\in\mathbf{M},\quad i^2\equiv -1\,(\mathrm{mod}\,p)\right\}.$$

В этом случае условие делимости имеет вид $N|(p^2-1)$ и, в силу равенства

$$(p^2-1)=(p-1)(p+1)=2^{q+1}\left(2^{q-1}-1\right),$$

в поле $\mathbf{M}(i)$ существуют корни степени $N=2^t,\quad (t=1,2,\ldots,q+1)$.

Следует отметить, что арифметические действия в поле $\mathbf{M}(i)$ совершено аналогичны операциям в комплексном поле $\mathbf{C}$ и отличаются лишь необходимостью вычисления остатков по $(\mathrm{mod}\,p)$. В разделе 1.3.2 мы рассматриваем также специфические системы счисления в поле $\mathbf{M}(i)$, позволяющие еще более упростить некоторые операции над элементами этого поля.

1.2.2. Арифметика в полях по модулю числа Ферма

Простым числом Ферма называется простое число вида

$$f=f_k=2^{2^k}+1=2^B+1,\quad k=0,1,2,3,4.$$

В настоящее время известны только эти простые указанного вида и неизвестно, конечно ли их количество. В задачах цифровой обработки сигналов наиболее часто используется четвертое простое число Ферма, равное $f_4=2^{2^4}+1=2^{16}+1=65537$.

Сформулируем основные правила вычислений в поле $\mathbf{F} \cong \mathbf{Z}/f\mathbf{Z}$, $f = 2^B + 1$:

1) любой элемент поля $\mathbf{F}$ *представляется в форме*

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_B 2^B, \quad x_j \in \{0,1\}; \tag{1.6}$$

2) это представление для всех $2^B \neq x \in \mathbf{F}$ *имеет вид*

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{B-1} 2^{B-1} + 0 \cdot 2^B;$$

3) "исключительный" нулевой элемент представим в форме:

$$2^B = 0 \cdot 2^0 + 0 \cdot 2^1 + \ldots + 0 \cdot 2^{B-1} + 1 \cdot 2^B;$$

4) *так как* $2^B \equiv -1 \pmod{f}$, *то в случае возникновения "бита переполнения"* $1 \cdot 2^B$ *при вычислениях эта единица, в случае "неисключительного" результата, переносится в "самый младший разряд" и вычитается из полученного числа;*

5) умножение элемента $x \in \mathbf{F}$ *на элемент* $2 \in \mathbf{F}$ *равносильно циклическому сдвигу "цифр"* x_j *в представлении* (1.6) *с инверсией знака в младшем разряде:*

$$2x = (-x_B) \cdot 2^0 + x_0 \cdot 2^1 + \ldots + x_{B-1} 2^B;$$

6) *умножение элементов поля* $\mathbf{F}$ *"столбиком" сводится к циклическим перестановкам цифр и сложениям-вычитаниям*;

7) *мультипликативный порядок элемента* $2 \in \mathbf{F}$ *равен 2B:* $\mathbf{Ord}(2) = 2B$ *(следовательно, для* $\omega = 2 \in \mathbf{F}$ *возможна реализация ТЧП* (1.3) *длины N = 2B без умножений).*

Следует отметить, что относительными недостатками чисел Ферма является более сложная реализация арифметических операций в поле $\mathbf{F}$ по сравнению с мерсенновским полем $\mathbf{M}$: наличие "исключительного" элемента, необходимость вычитания, а также то, что простых Ферма известно мало. Но эти недостатки несколько компенсируются тем фактом, что условие делимости $N \mid (f - 1)$ име-

ет вид $N \mid 2^B$ и, следовательно, в поле $\mathbf{F}$ существуют корни степени $N = 2^t \quad (t = 1,2,\ldots,B)$.

1.2.3. Арифметика в полях по модулю числа Голомба

Простым числом Голомба будем называть простое число вида

$g = g_k = 3 \cdot 2^k + 1 = 2^{k+1} + 2^k + 1$.

В частности, простыми числами Голомба являются числа

$g_8 = 769, \qquad g_{30} = 3\,221\,225\,473,$

$g_{12} = 12\,289, \qquad g_{36} = 206\,158\,430\,209,$

$g_{18} = 786\,433, \qquad g_{41} = 6\,597\,069\,776\,657.$

Сформулируем основные правила вычислений в поле $\mathbf{G} \cong \mathbf{Z}/g\mathbf{Z}$, $g = g_k = 2^{k+1} + 2^k + 1$:

1) любой элемент поля $\mathbf{G}$ *представляется в форме*

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{k+1} 2^{k+1}, \quad x_j \in \{0,1\}; \tag{1.7}$$

2) *так как*

$$2^{k+1} \equiv -2^k - 1 \pmod{g}, \tag{1.8}$$

то в случае возникновения "бита переполнения" $1 \cdot 2^{k+1}$ *при вычислениях эта единица, в случае необходимости, переносится и вычитается дважды согласно* (1.8)*;*

3) *умножение элемента* $x \in \mathbf{G}$ *на элемент* $2 \in \mathbf{G}$ *сводится к циклическим перестановкам цифр* x_j *в представлении* (1.7) *и сложениям-вычитаниям*;

4) *умножение элементов поля* $\mathbf{G}$ *"столбиком" также сводится к циклическим перестановкам цифр и сложениям-вычитаниям*;

5) *мультипликативный порядок элемента* $2 \in \mathbf{G}$ *равен* $3 \cdot 2^{k-1}$*:* $\mathbf{Ord}(2) = 3 \cdot 2^{k-1}$ *(следовательно, при* $\omega = 2 \in \mathbf{G}$ *возможна реализация ТЧП* (1.3) *длины* $N = 3 \cdot 2^{k-1}$ *без умножений);*

6) *мультипликативный порядок элемента* $8 \in \mathbf{G}$ *равен* 2^{k-1}: $\mathbf{Ord}(2^3) = 2^{k-1}$ *(следовательно, при* $\omega = 2^3 \in \mathbf{G}$ *возможна реализация ТЧП* (1.3) *длины* $N = 2^{k-1}$ *без умножений).*

Несмотря на наличие корней ω "удобной" степени $N = 2^{k-1}$, арифметические операции в поле $\mathbf{G}$ имеют более сложную реализацию при представлении элементов поля в "модулярной" двоичной системе счисления в форме (1.7). Это связано в первую очередь с необходимостью одновременного или последовательного вычитания для двух разрядов представления (1.7), причем каждое из этих вычитаний может также привести к переполнению разрядной сетки. В разделе 1.3.1 мы рассмотрим некоторые методы преодоления отмеченных трудностей.

1.3. Редуцированные системы счисления в конечных полях

1.3.1. Двоично-избыточная система счисления

Рассмотренные выше примеры реализации модулярных вычислений для модулей специального вида (Мерсенна, Ферма, Голомба) используют некоторую модификацию обычной двоичной системы счисления, причем реализация модулярной арифметики будет тем эффективнее, чем меньше возникает специфических отличий, связанных с нахождением вычета целого числа по $(\mathrm{mod}\, p)$. Эти имеющиеся отличия "двоичных" вычислений в конечных полях (кольцах) определяют специфические правила "переноса в старший разряд", то есть своеобразие двоичной модулярной арифметики, двоичной модулярной системы счисления. Позиционные системы счисления в конечных кольцах будем называть далее *редуцированными системами счисления*.

Следует отметить, что для вычислений по модулю чисел Ферма и, в особенности Голомба, при умножении на степень двойки приходится производить вычитание, так как простая инверсия знаков

одного или нескольких бит выводит вычисления за рамки двоичности. Если допустить "законность" цифр $\{-1,0,1\}$, сохраняя при этом двоичное основание системы, то получается редуцированная система счисления, в которой элементы кольца классов вычетов, например, по модулю числа Ферма $f = 2^B + 1, \quad (B = 2b)$ представляются неоднозначно в форме

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_B 2^B, \quad x_j \in \{-1,0,1\}. \qquad (1.9)$$

Отмеченную избыточность представления (1.9) можно несколько уменьшить, заметив, что справедливы соотношения:

$$0 \le x_0 2^0 + x_1 2^1 + \ldots + x_{b-1} 2^{b-1} < 2^b, \quad x_j \in \{0,1\},$$

$$-2^b < x_0 2^0 + x_1 2^1 + \ldots + x_{b-1} 2^{b-1} \le 0, \quad x_j \in \{-1,0\},$$

а также то, что любое целое число из промежутка $\left(-2^b, 0\right]$ сравнимо по $(\mathrm{mod}\, f)$ с некоторым целым числом из промежутка $\left[2^b, f\right)$ и наоборот. Аналогичные соображения справедливы и для элементов кольца классов вычетов по модулю чисел Голомба.

Конечно, добиться полной однозначности представления не удается. Действительно, в рассмотренном случае поля по $(\mathrm{mod}\, f)$ справедливы, например, равенства

$$1 \cdot 2^2 + (-1) \cdot 2^0 = 3 = 1 \cdot 2^1 + 1 \cdot 2^0.$$

Пример 1.1. Пусть g есть простое число Голомба, элемент $x \in \mathbf{G}$ запишем в виде

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{k-3} 2^{k-3} + \delta_1 2^{k-2} + \ldots + \delta_4 2^{k+1},$$

а элемент $8x \in \mathbf{G}$ - в виде

$$2^3 x = y_1 2^0 + y_2 2^1 + y_3 2^2 + x_0 2^3 + \ldots + x_{k-3} 2^k + y_4 2^{k+1}.$$

В таблице 1.1 указано соответствие между "цифрами" $\delta_1, \ldots \delta_4$ элемента x и "цифрами" $y_1, \ldots y_4$ 'элемента $8x \in \mathbf{G}$ для представления в двоично-избыточной системе счисления.

Таблица 1.1

δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4	δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4	δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4
0	0	0	0	0	0	0	0	1	0	0	0	-1	1	-1	1	-1	0	0	0	1	-1	1	-1
0	0	0	1	1	0	0	0	1	0	0	1	0	1	-1	1	-1	0	0	1	-1	-1	1	0
0	0	0	-1	-1	0	0	0	1	0	0	-1	1	1	-1	0	-1	0	0	-1	0	-1	1	-1
0	0	1	0	-1	0	0	1	1	0	1	0	1	1	0	-1	-1	0	1	0	0	-1	1	0
0	0	1	1	0	0	0	1	1	0	1	1	-1	1	0	0	-1	0	1	1	1	-1	1	0
0	0	1	-1	1	0	0	0	1	0	1	-1	-1	1	0	-1	-1	0	1	-1	-1	-1	1	0
0	0	-1	0	1	0	0	-1	1	0	-1	0	0	1	-1	0	-1	0	-1	0	-1	-1	0	1
0	0	-1	1	-1	0	0	0	1	0	-1	1	1	1	-1	0	-1	0	-1	1	1	-1	0	1
0	0	-1	-1	0	0	0	-1	1	0	-1	-1	-1	1	-1	0	-1	0	-1	-1	1	-1	0	0
0	1	0	0	1	0	1	-1	1	1	0	0	0	1	0	0	-1	1	0	0	-1	-1	1	1
0	1	0	1	-1	0	1	0	1	1	0	1	1	1	0	0	-1	1	0	1	1	-1	1	1
0	1	0	-1	0	0	1	-1	1	1	0	-1	-1	1	0	0	-1	1	0	-1	1	-1	1	0
0	1	1	0	0	0	1	0	1	1	1	0	-1	1	0	1	-1	1	1	0	1	-1	1	0
0	1	1	1	1	0	1	0	1	1	1	1	0	1	0	1	-1	1	1	1	1	0	0	0
0	1	1	-1	-1	0	1	0	1	1	1	-1	1	1	0	0	-1	1	1	-1	-1	-1	1	0
0	1	-1	0	-1	0	0	1	1	1	-1	0	1	1	-1	0	-1	1	-1	0	1	-1	1	0
0	1	-1	1	0	0	0	1	1	1	-1	1	-1	1	0	0	-1	1	-1	1	1	0	0	0
0	1	-1	-1	1	0	0	0	1	1	-1	-1	0	1	0	-1	-1	1	-1	-1	-1	-1	1	0
0	-1	0	0	-1	0	-1	-1	1	-1	0	0	1	1	-1	-1	-1	-1	0	0	0	-1	0	0
0	-1	0	1	0	0	-1	1	1	-1	0	1	-1	1	-1	0	-1	-1	0	1	1	-1	0	0
0	-1	0	-1	1	0	-1	0	1	-1	0	-1	-1	1	-1	-1	-1	-1	0	-1	-1	-1	0	0

1.3.2. Редуцированные системы счисления в комплексном поле Мерсенна

Редуцированные системы счисления с "нетрадиционными" основаниями могут быть рассмотрены и для алгебраических расширений конечных полей.

Приводимый ниже пример целиком заимствован из книги [3].

Пример 1.2. Выбор основания $2i$ приводит к системе счисления, которую естественно назвать "мнимо-четверичной" (по аналогии с "четверичной") ввиду того, что каждое комплексное число может быть представлено в этой системе при помощи цифр $0,1,2,3$, причем тех же цифр, взятых со знаком минус, не требуется). Например,

$$(11210.31)_{2i} =$$

$$= 1\cdot 16 + 1\cdot(-8i) + 2\cdot(-4) + 1\cdot(-2i) + 3\cdot\left(-\frac{1}{2}i\right) + 1\cdot\left(-\frac{1}{4}\right) =$$

$$= 7\frac{3}{4} - 7\frac{1}{2}i$$

Так как справедливо равенство

$$(a_{2n}\ldots a_1 a_0 .\ a_{-1}\ldots a_{-2k})_{2i} =$$

$$= (a_{2n}\ldots a_2 a_0 .\ a_{-2}\ldots a_{-2k})_{-4} + \quad ,$$

$$+2i(a_{2n-1}\ldots a_3 a_1 .\ a_{-1}\ldots a_{-2k+1})_{-4}$$

то перевод числа в мнимо-четверичную форму и обратно сводится к переводу в "негативно-четверичную" форму и обратно. Интересное свойство этой системы состоит в том, что она допускает выполнение умножения и деления комплексных чисел целостным образом без раздельного рассмотрения вещественных и мнимых частей. Например, перемножить два числа мы можем в этой системе так же, как и при любом другом основании, используя только несколько иное "правило переноса". В случае если цифра становится

больше 4, мы вычитаем 4 и "переносим" (–1) на два столбца влево, а когда получается отрицательная цифра, мы прибавляем к ней 4 и "переносим" (+1) на два столбца влево. Разбор нижеследующего примера пояснит, как работает это своеобразное правило переноса:

$$
\begin{array}{rl}
12231 & [9-10i] \\
12231 & [9-10i] \\
\hline
12231 & \\
10320213 & \\
13022 & \\
13022 & \\
12231 & \\
\hline
021333121 & [-19-180\ \ i]
\end{array}
$$

Пусть $\mathbf{M} \cong \mathbf{Z}/p\mathbf{Z}$, и $p = 2^q - 1$ является простым числом Мерсенна. Рассмотрим "модулярный" аналог этой системы счисления для "комплексного поля Мерсенна"

$$\mathbf{M}(i) = \left\{ z : a + bi;\ a, b \in \mathbf{M},\quad i^2 \equiv -1 \,(\mathrm{mod}\, p) \right\}.$$

Лемма 1.1. *Любой элемент* $z \in \mathbf{M}(i)$ *может быть представлен в форме*

$$z = a_{-1}(2i)^{-1} + a_0(2i)^0 + a_1(2i)^1 + \ldots + a_\nu(2i)^\nu,\ a_j = 0,1,2,3, \qquad (1.10)$$

где $\nu = \nu(q) = q - 1$.

Доказательство. Положим

$$z = x - (2i)^{-1}(2y') = x - (2i)^{-1} y;\ x, y \in \mathbf{M}\ , \qquad (1.11)$$

где

$$
\begin{aligned}
&x \equiv x_0(-4)^0 + x_2(-4)^1 + \ldots + x_{2t}(-4)^t \,(\mathrm{mod}\, p), \\
&y \equiv y_0(-4)^0 + y_2(-4)^1 + \ldots + y_{2t}(-4)^t \,(\mathrm{mod}\, p), \qquad (1.12) \\
&x_j, y_j \in \{0,1,2,3\}.
\end{aligned}
$$

Тогда доказательство леммы сводится к доказательствам:

(а) принципиальной возможности представления элементов поля **M** в форме (1.12),

(б) определению минимального натурального $t=t(p)$ при котором возможно такое представление.

Для доказательства утверждений (а)-(б) достаточно заметить, что представление произвольного элемента поля **M** в четверичной системе счисления возможно и требует не более $t = {(q+1)}/{2}$ слагаемых. Далее, так как

$$x \equiv x_0(-4)^0 + x_2(-4)^1 + \ldots + x_{2t}(-4)^t \pmod p \equiv$$
$$\equiv \left(x_0(4)^0 + x_4(4)^2 + \ldots\right) - 4\left(x_2(4)^0 + x_6(4)^2 + \ldots\right) \pmod p \equiv$$
$$\equiv X^{(+)} - 4X^{(-)} \pmod p, \quad X^{(+)}, X^{(-)} \in \mathbf{M},$$

то и для элемента $X^{(+)} - 4X^{(-)} \in \mathbf{M}$ также требуется не более $t = {(q+1)}/{2}$ слагаемых.

Находя для элементов $x, y \in \mathbf{M}$ их представление в "негачетверичной" системе счисления (системе счисления с основанием (-4)) и полагая далее в соответствии с равенством (1.11)

$$a_{-1} = y_0, a_0 = x_0, a_1 = y_1, a_2 = x_1 \ldots$$

получаем утверждение Леммы 1.2. ♦

Лемма 1.2. *Мультипликативный порядок элемента 2i в поле* $\mathbf{M}(i)$ *равен* $\mathbf{Ord}\,(2i) = 4q$.

Доказательство. Вычисляя последовательно, получаем:

$(2i)^2 = -4, \quad (2i)^4 = 16$.

Далее, в силу того, что н.о.д$\left(16, 2^q - 1\right) = 1$, мультипликативный порядок элемента $16 = 2^4$ равен мультипликативному порядку эле-

мента 2 и , следовательно, для элемента $2i$ в поле $\mathbf{M}(i)$ справедливо соотношение:

$$\mathbf{Ord}\,(2i) = 4\mathbf{Ord}\,(16) = 4\mathbf{Ord}\,(2) = 4q\,. \qquad \blacklozenge$$

Таким образом, для $\omega = 2i$ возможна реализация ТЧП длины $N = 4q$ без умножений в поле $\mathbf{M}(i)$.

Как и в комплексном случае, при сложении и умножении элементов поля $\mathbf{M}(i)$ в редуцированной мнимо-четвертичной системе счисления в промежуточных результатах могут возникнуть "цифры", не являющиеся элементами множества $\{0,1,2,3\}$. Другими словами, необходимо сформулировать "правила переноса" в старшие разряды для действий, производимых над элементами в форме (1.12). Сформулируем эти непосредственно проверяемые правила в виде леммы.

Лемма 1.3. *В поле* $\mathbf{M}(i)$ *справедливы равенства:*

$$4 = 1\cdot(2i)^4 + 3\cdot(2i)^2 = 1\cdot(-4)^2 + 3\cdot(-4)^1 =,$$
$$5 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 1\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 1\cdot(-4)^0,$$
$$6 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 2\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 2\cdot(-4)^0,$$
$$7 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 3\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 3\cdot(-4)^0,$$
$$8 = 1\cdot(-4)^2 + 2\cdot(-4)^1,$$
$$9 = 1\cdot(-4)^2 + 2\cdot(-4)^1 + 1\cdot(-4)^0.$$

$\blacklozenge$

Несмотря на "четверичность" рассмотренной системы счисления, вычисления в ней легко реализуются на обычное "бинарной" вычислительной технике, если рассмотреть для каждого из возможных значений "цифр" $a_j = 0,1,2,3$ их двухбитовое представление.

"Бинарную" редуцированную систему счисления для поля $\mathbf{M}(i)$ можно также получить, используя основание $i-1$, рассматриваемую более подробно в третьей части пособия.

Лемма 1.4. *Любой элемент* $z \in \mathbf{M}(i)$ *может быть представлен в форме*

$$z = a_0(i-1)^0 + a_1(i-1)^1 + \ldots + a_\nu(i-1)^\nu, a_j = 0,1, \qquad (1.13)$$

где $\nu = \nu(q) \le 8\left(\left[q/4\right]+1\right)$.

Доказательство. Положим $i-1=\alpha$. Так как $\alpha^8 = 16$, то для элемента $z \in \mathbf{M}(i)$ справедливо представление в шестнадцатеричной системе счисления

$$z = b_0 16^0 + b_1 16^1 + \ldots + b_\mu 16^\mu, b_j = 0,1,\ldots,15,$$

где $\mu = \left[q/4\right]+1$. В свою очередь, шестнадцатиричные "цифры" b_j представляются в виде сумм степеней элемента $i-1=\alpha$, что и доказывает Лемму 1.4. ♦

Как и в случае мнимо-четверичной системы счисления, при сложении и умножении элементов поля $\mathbf{M}(i)$ в редуцированной системе счисления в промежуточных результатах может возникнуть "цифра", не являющаяся элементом множества $\{0,1\}$. В этом случае "правило переноса" в старшие разряды для действий, производимых над элементами поля $\mathbf{M}(i)$, определяется соотношением

$$2\cdot(i-1)^0 = (i-1)^3 + (i-1)^2.$$

Лемма 1.5. *Мультипликативный порядок элемента* $(i-1)$ *в поле* $\mathbf{M}(i)$ *равен* $\mathbf{Ord}\,(i-1) = 8q$.

Доказательство. Так как $(i-1)^2 = -2i$, то справедливо равенство

$$\mathbf{Ord}\,(i-1) = 2\mathbf{Ord}\,(-2i) = 2 \cdot 4q = 8q\,. \qquad \blacklozenge$$

Таким образом, для $\omega = (i-1)$ возможна реализация ТЧП длины $N = 8q$ без умножений в поле.

1.4. Алгоритмы вычисления свертки в полях p-адических чисел

1.4.1. p-адические числа

Пусть p – простое число. Пусть $v_p(a)$ есть *p-адический показатель целого числа a*, т.е. наибольшее неотрицательное число m, для которого $a \equiv 0 \pmod{p^m}$. Для рационального числа $x = \frac{a}{b}$ показатель $v_p(x)$ принимается равным

$$v_p(x) = v_p(a) - v_p(b)\,.$$

Далее, p-адическая норма $\|x\|_p$ на множестве рациональных чисел определяется равенством

$$\|x\|_p = \begin{cases} p^{-v_p(x)}, & \text{если} \quad x \neq 0; \\ 0, & \text{если} \quad x = 0, \end{cases} \tag{1.14}$$

а p-адическая метрика равенством

$$\rho_p(x, y) = \|x - y\|_p\,; \quad x, y \in \mathbf{Q}\,.$$

Легко проверяется, что равенство (1.14) действительно задает в поле **Q** норму, причем "неравенство треугольника"

$$\|x + y\|_p \leq \|x\|_p + \|y\|_p$$

выполняется в форме

$$\|x+y\|_p \le \max\left\{\|x\|_p, \|y\|_p\right\}. \qquad (1.15)$$

(Нормы с условием (1.15) называются *неархимедовыми нормами*).

Наряду с неархимедовыми нормами мы будем также рассматривать и "традиционную" архимедову норму в поле **Q,** равную абсолютной величине (модулю) числа, которую будем обозначать $|x| = \|x\|_\infty$. Пополнение поля **Q,** согласно общей схеме [4], [5], относительно нормы $|x| = \|x\|_\infty$ приводит к вещественным числам **R,** пополнение поля **Q** относительно нормы $\|x\|_p$ приводит к полю так называемых p-адических чисел $\mathbf{Q}_p$. [6].

Произвольный элемент $b \in \mathbf{Q}_p$ может быть записан в виде p-адического разложения

$$b = \frac{b_{-m}}{p^m} + \ldots + \frac{b_{-1}}{p} + b_0 + b_1 p + b_2 p^2 + \ldots \qquad (1.16)$$

с целыми "цифрами" b_j ($0 \le b_j < p$; $b_{-m} \ne 0$) и конечным числом отрицательных степеней p^j в (1.16). Если в соотношении (1.16) $(-m) > 0$, то элемент $b \in \mathbf{Q}_p$ называется целым p-адическим числом, кольцо которых обозначается $\mathbf{Z}_p$; в отличие кольца от целых p-адических чисел $\mathbf{Q}_p$, кольцо "обычных" целых $\mathbf{Z} \subset \mathbf{Q}_p$, для которых в представлении (1.16) лишь конечное число слагаемых отлично от нуля и $(-m) > 0$, будем называть кольцом целых рациональных чисел.

Распространим понятие p-адического показателя на все множество p-адических чисел $\mathbf{Q}_p$, полагая $v_p(x) = -m$ для числа x в представлении (1.16). В терминах такого продолжения показателя

$v_p(x)$ равенствами (1.14) и (1.16) естественно продолжаются на поле $\mathbf{Q}_p$ и p-адическая норма, и p-адическая метрика. Кроме того, для $a,\ b \in \mathbf{Q}_p$ сравнение $a \equiv b \pmod{p^r}$ будем понимать как

$$\|a-b\|_p \le p^{-r}, \tag{1.17}$$

что согласуется с обычным определением сравнимости $\pmod{p^r}$ целых рациональных чисел. Соотношение (1.8) представляет собой метрическую интерпретацию сравнимости чисел в " p-адической шкале": два целых числа тем p-адически ближе, чем на большую степень числа p делится их разность.

Замечание 1.1. Неподготовленного читателя не должна шокировать запись (1.16) представления p-адического числа в виде "расходящегося" ряда ("общий член ряда не стремится к нулю!"). С рядом все в порядке: и p-адическая норма общего члена стремится к нулю, и сходится он. Только сходимость понимается в смысле сходимости по p-адической норме.

Для удобства ссылок сформулируем ряд известных свойств поля p-адических чисел $\mathbf{Q}_p$ в форме леммы.

Лемма 1.6. *(а) всякое целое p-адическое число сравнимо с целым рациональным числом* $\pmod{p^r}$;

(б) всякое p-адическое число сравнимо с некоторым рациональным числом $\pmod{p^r}$;

(в) классы сравнимых $\pmod{p^r}$ *целых p-адических чисел образуют покрытие* $\mathbf{Z}_p$ *непересекающимися "шарами" p-адического диаметра* p^{-r} *(в каждом таком шаре найдется целый рациональный представитель);*

(г) фактор-кольцо $\mathbf{Z}_p$ *по отношению сравнимости* $(\mathrm{mod}\ p^r)$ *изоморфно кольцу классов вычетов* $\mathbf{Z}(\mathrm{mod}\ p^r)$*;*

(д) целые p-адические числа с нормой, меньшей p^{-r}*, образуют идеал в кольце* $\mathbf{Z}_p$*.* ♦

Замечание 1.2. При "приближенном", то есть в смысле арифметики по $(\mathrm{mod}\ p^r)$, сложении и умножении p-адических чисел p-адическая погрешность, в отличие от вещественного случая, не увеличивается (утверждение (д) Леммы 1.6).

Сказанное выше позволяет сделать важный вывод о том, что многие алгоритмы вычисления свертки (1.1), основанные на применении ДПФ в кольцах классов вычетов, то есть ТЧП, можно интерпретировать как приближенные вычисления свертки в неархимедово нормированном поле $\mathbf{Q}_p$. Вычислительная погрешность в ряде случаев может быть компенсирована за счет имеющейся априорной информации об ожидаемом результате (целочисленность, вещественность, ограниченность).

1.4.2. Вычисление свертки с помощью ТЧП по модулю степени простого числа

Для "безошибочного" вычисления свертки спектральным методом с использованием ТЧП, число p должно быть достаточно велико – удовлетворять неравенству (1.4), что ограничивает возможности использования модулей специального вида, для которых известны эффективные реализации арифметических операций.

Пример 1.3. Пусть $f_4 = 2^{16} + 1$ есть четвертое простое число Ферма. При решении достаточно типичной для цифровой обработки изображений задачи вычисления двумерной свертки двух цело-

численных массивов размера (512×512) с диапазонами изменения значений $0 \div 255$, для числа p должно выполняться неравенство:

$$p > (512)^2 \ (256)^2 = 2^{34} > f_4 = 2^{16} + 1.$$

Это существенно ограничивает возможности применения, например, ТЧП Ферма в задачах обработки многомерной цифровой информации.

Использование в качестве модулей в преобразовании (1.3) составных чисел добавляет серьезные трудности, связанные с существованием в модулярных кольцах по составным модулям делителей нуля и, как следствие, с необратимостью некоторых элементов соответствующих колец и/или с неортогональностью базисных функций преобразования (1.3). Действительно, доказательство ортогональности базисных функций дискретного преобразования Фурье длины N сводится к проверке равенства

$$\sum_{n=0}^{N-1} \omega^{mn} \omega^{-nk} = \begin{cases} \dfrac{1-\omega^{N(m-k)}}{1-\omega^{(m-k)}} = 0, & \text{при } m \neq k \ (\mathrm{mod}\, N); \\ N, & \text{при } m \equiv k \ (\mathrm{mod}\, N). \end{cases} \qquad (1.18)$$

Доказательство последнего соотношения представляет собой тривиальное упражнение на суммирование геометрической прогрессии и остается справедливым и для случая конечного поля, в котором существует корень степени N из единицы. Условие "быть полем", то есть простота модуля в (1.3), существенна. В поле только нулевой элемент необратим, что гарантирует возможность "деления" на элемент $\left(1-\omega^{(m-k)}\right)$ в первой строчке равенства (1.18). При составном модуле элемент $\left(1-\omega^{(m-k)}\right)$ в соотношении (1.18) может быть необратимым и для несравнимых по (mod N) значений m,k . Таким образом, вложение поля $\mathbf{Q}$ в поле $\mathbf{Q}_p$ и рассмотрение аналога ДПФ в поле $\mathbf{Q}_p$ в принципе решает проблему с ор-

тогональностью базисных функций, но вынуждает использовать для их значений бесконечные представления (1.16).

В действительности, при наличии априорной информации о диапазоне изменения значений сворачиваемых функций, никаких вычислений с бесконечными представлениями не производится. В самом деле, пусть p - простое нечетное число. Тогда мультипликативная группа обратимых элементов кольца классов вычетов $\left(\mathrm{mod}\ p^r\right)$ циклична и имеет порядок $p^{r-1}\left(p-1\right)$. Следовательно, при любом натуральном r в кольце $\mathbf{Z}_p$ существуют первообразные корни ω из единицы степени N с условием $N\left|\left(p-1\right)\right.$. Тогда применение пары взаимно обратных преобразований

$$\hat{x}\left(m\right)=\sum_{n=0}^{N-1}x\left(n\right)\ \ \omega^{mn}\ , \tag{1.19}$$

$$x\left(k\right)=\frac{1}{N}\sum_{m=0}^{N-1}\hat{x}\left(m\right)\ \ \omega^{k(N-m)} \tag{1.20}$$

позволяет найти свертку (1.1) как элемент кольца $\mathbf{Z}_p$.

Пусть r таково, что целочисленный результат свертки (1.1) удовлетворяет неравенству $0\le z\left(k\right)<p$. Пусть ω_r такое целое рациональное число, существующее по условию (в) Леммы 1.6, что $\left\|\omega-\omega_r\right\|_p<p^{-r}$.

Применение для вычисления свертки вместо преобразований (1.19) и (1.20), преобразований

$$\hat{x}_r\left(m\right)=\sum_{n=0}^{N-1}x\left(n\right)\ \ \omega_r^{mn}\ , \tag{1.21}$$

$$x_r\left(k\right)=\frac{1}{N}\sum_{m=0}^{N-1}\hat{x}_r\left(m\right)\ \ \omega_r^{k(N-m)} \tag{1.22}$$

позволяет найти "приближенное" целочисленное значение $z_r(k)$ свертки с p-адической точностью $\varepsilon<p^{-r}$, то есть с точностью до

целого слагаемого, делящегося на число p^r. С учетом априорной информации об ограниченности $z(k)$ получается точный результат: $z_r(k) = z(k)$.

1.4.3. Реализация арифметических операций в кольце классов вычетов по модулю степени числа Мерсенна

В свете содержания предыдущего раздела, возможность и целесообразность вычисления свертки в кольце классов вычетов по модулю степени простого числа не вызывает особых сомнений. Принципиальным остается вопрос об эффективности реализации арифметических операций в случае специального вида простого числа (Мерсенна, Ферма и т.п.).

Пусть p –число Мерсенна: $p = 2^q - 1$ (не обязательно простое), k – натуральное, $\mathbf{K} = \mathbf{Z}/p^k\mathbf{Z}$ -кольцо классов вычетов $(\mathrm{mod}\, p^k\mathbf{Z})$. Тогда элемент $X \in \mathbf{K}$ может быть представлен в форме

$$X = X_0 + X_1 p^1 + \ldots + X_{k-1} p^{k-1}, \qquad (1.23)$$

где, в свою очередь, элементы

$$X_j : 0 \le X_j \le p-1; \quad j = 0,1,\ldots,k-1$$

представимы в "битовой" мерсенновской форме:

$$X_j = x_{j0} + x_{j1} 2^1 + \ldots + x_{j,q-1} 2^{q-1}. \qquad (1.24)$$

Эффективность реализации арифметических операций над элементами из $\mathbf{K}$ определяется эффективностью реализации правил переноса "битов переполнения" для "блоков" X_j $(j = 0,1,\ldots,k-1)$, возникающих при сложении и умножении элементов в форме (1.23). При $k = 1$ такие правила описаны в разделе 1.2.1. Пусть $k \ge 1$. Тогда из очевидного равенства

$$2^q = 1 \cdot \left(2^q - 1\right) + 1$$

легко следует формулировка "правила переноса битов переполнения":

- *внутри каждого из "блоков"* X_j *перенос в старший разряд осуществляется по обычным правилам битовой арифметики Мерсенна;*
- *при возникновении "бита переполнения"* $1 \cdot 2^q$ *для блоков* X_j $(j = 0,1,\ldots,k-2)$, *единица q-го разряда "раздваивается": одна из единиц суммируется с элементом* X_{j+1}, *а вторая суммируется с элементом* X_j;
- *при возникновении "бита переполнения"* $1 \cdot 2^q$ *для блока* X_{k-1} *единица q-го разряда суммируется с элементом* X_{k-1}.

1.4.4. Реализация арифметических операций в кольце классов вычетов по модулю степени числа Ферма

Реализация арифметических операций в кольце классов вычетов по модулю степени числа Ферма имеет некоторые особенности, отличия от рассмотренного выше случая степени числа Мерсенна. Это связано с тем, что "почти все" элементы кольца $\mathbf{K} = \mathbf{Z}/f\mathbf{Z}$ могут быть представлены в b-битовой форме

$$X = x_0 + x_1 2^1 + \ldots + x_{b-1} 2^{b-1} + 0 \cdot 2^b,$$

кроме одного элемента, представимого в $(b+1)$-битовой форме

$$2^b = 0 + 0 \cdot 2^1 + \ldots + 0 \cdot 2^{b-1} + 1 \cdot 2^b. \qquad (1.25)$$

Наличие в кольце $\mathbf{K} = \mathbf{Z}/f\mathbf{Z}$ "исключительного" элемента, равного 2^b, несколько усложняет и "правила переноса битов переполнения" для операций в кольце классов вычетов по модулю степени числа Ферма.

Пусть f –число Ферма: $f = 2^b + 1$ (не обязательно простое), k – натуральное, $\mathbf{K} = \mathbf{Z} \big/ f^k \mathbf{Z}$ - кольцо классов вычетов $(\mathrm{mod}\, f^k \mathbf{Z})$. Тогда элемент $X \in \mathbf{K}$ может быть представлен в "блочной" форме

$$X = X_0 + X_1 f^1 + \ldots + X_{k-1} f^{k-1},$$

где, в свою очередь, элементы

$$X_j : 0 \le X_j \le f - 1; \quad j = 0,1,\ldots,k-1 \tag{1.26}$$

представимы в "битовой" форме:

$$X_j = x_{j0} + x_{j1} 2^1 + \ldots + x_{j,b-1} 2^{b-1} + x_{jb} 2^b . \tag{1.27}$$

Пусть $k \ge 1$. Тогда из очевидного равенства

$$2^b = 1 \cdot \left(2^b + 1\right) - 1$$

следует формулировка "правила переноса битов переполнения":

- *внутри каждого из "блоков" X_j перенос в старший разряд осуществляется по обычным правилам битовой арифметики Ферма;*
- *при возникновении "бита переполнения" $1 \cdot 2^b$ для блоков X_j $(j = 0,1,\ldots,k-2)$, для "неисключительныых" значений X_j единица b-го разряда "раздваивается": одна из единиц суммируется с X_{j+1}, а вторая вычитается из X_j;*
- *при возникновении "бита переполнения" $1 \cdot 2^b$ для блока X_{k-1} для "неисключительныых" значений X_{k-1} единица b-го разряда вычитается из элемента X_{k-1};*
- *при возникновении "бита переполнения" $1 \cdot 2^b$ для блоков X_j $(j = 0,1,\ldots,k-1)$, для "исключительныых" значений X_j значение X_j не изменяется.*

1.5. Алгоритмы вычисления свертки в расширениях неархимедово нормированных полей

1.5.1. Продолжение p-адических нормирований на квадратичные расширения поля **Q**

Рассмотрим квадратичное расширение $\mathbf{Q}\left(\sqrt{d}\right)$, где число d свободно от квадратов (то есть не делится на квадрат натурального, отличного от единицы):

$$\mathbf{Q}\left(\sqrt{d}\right)=\left\{z=x+y\sqrt{d};\, x,y\in\mathbf{Q}\right\}.$$

Дискриминант этого поля равен $4d$. Пусть p – простое число с условием

$$4d\neq 0 \pmod p. \tag{1.28}$$

Для удобства ссылок сформулируем известные факты (см. [7]) о продолжении p-адических нормирований поля **Q** на расширение $\mathbf{Q}\left(\sqrt{d}\right)$ в форме отдельных лемм.

Лемма 1.7. *Если d является квадратичным невычетом* $\pmod p$, *то функция*

$$\Phi_p(z)=\Phi_p\left(x+y\sqrt{d}\right)=\sqrt{\left\|x^2-dy^2\right\|_p} \tag{1.29}$$

продолжает p-адическое нормирование поля **Q** *на расширение* $\mathbf{Q}\left(\sqrt{d}\right)$. ♦

Лемма 1.8. *Если d является квадратичным вычетом* $\pmod p$, *то функция*

$$\Psi_p^{\pm}(z)=\left\|x\pm\lambda y\right\|_p, \tag{1.30}$$

где λ есть p-адическое решение уравнения $w^2=d$, продолжает p-адическое нормирование поля **Q** *на расширение* $\mathbf{Q}\left(\sqrt{d}\right)$. ♦

Лемма 1.9. *Если p – простое нечетное число с условием $d \equiv 0 \pmod{p}$, то функция* (1.29) *продолжает p-адическое нормирование поля* $\mathbf{Q}$ *на расширение* $\mathbf{Q}\left(\sqrt{d}\right)$. ♦

Лемма 1.10. *Если $p = 2$, то либо функция (1.29), либо функции (1.30) продолжают диадическое (2-адическое) нормирование поля* $\mathbf{Q}$ *на расширение* $\mathbf{Q}\left(\sqrt{d}\right)$ *в зависимости от того, неразложим или разложим многочлен $f(w) = w^2 - d$ на множители над полем* $\mathbf{Q}_2$ *соответственно.* ♦

1.5.2. Метрическая форма китайской теоремы об остатках

Китайская теорема об остатках позволяет при попарно взаимно простых $m_1, m_2, \ldots, m_t$ определять из системы сравнений

$$\begin{cases} x \equiv \beta_1 \pmod{m_1} \\ \quad \ldots \\ x \equiv \beta_t \pmod{m_t} \end{cases} \tag{1.31}$$

вычет числа $x \pmod{m_1 \ldots m_t}$:

$$x \equiv \beta = \sum_{j=1}^{t} a_j \beta_j M_j , \tag{1.32}$$

$$M = m_1 \ldots m_t, M_j = M \big/ m_j , \; a_j M_j \equiv 1 \pmod{m_j}.$$

Другими словами, если $m_j = p_j^{v_j}$, где p_j - различные простые числа, то равенство (1.32) утверждает существование целого числа x, удаленного от каждого из целых β_j в смысле p_j - адической метрики на расстояние, не большее чем $p_j^{v_j}$:

$$\begin{cases} |x-\beta_1|_{p_1} \le p_1^{-\nu_1} \\ \quad \dots \\ |x-\beta_t|_{p_t} \le p_t^{-\nu_t} \end{cases}.$$

Факт существования такого "аппроксимирующего" числа x имеет место и в случае, когда одна из норм $\|\bullet\|_{p_j}$ является архимедовой нормой $\|\bullet\|_\infty$.

Теорема 1.1. (аппроксимационная теорема для семейства нормирований [7]).

Пусть $\psi_1(\bullet)=\|\bullet\|_1,\dots,\psi_s(\bullet)=\|\bullet\|_s$ *- различные нормирования поля* **Q.** *Для заданных элементов* $\beta_1,\beta_2,\dots,\beta_t \in \mathbf{Q}$ *существует элемент* $\beta \in \mathbf{Q}$, *который расположен сколь угодно близко к элементу* β_j *относительно нормирования* ψ_j *:*

$$\psi_j(\beta-\beta_j)<\varepsilon.$$

1.5.3. Случай $\mathbf{Q}(\sqrt{d})$, *d – невычет (mod p)*

Рассмотрим частные случаи квадратичных расширений $\mathbf{Q}(\sqrt{d})$, когда d является невычетом (mod p). Пусть простое p подчинено условию $p \equiv 3 \pmod 4$ (например, p - простое число Мерсенна: $p=2^q-1$). Тогда, как известно [8],[9], число p не может быть представлено в виде суммы двух квадратов целых чисел и, в частности, многочлен $f(t)=t^2+1$ неприводим $(\mathrm{mod}\ p)$, (то есть (-1) является квадратичным невычетом $(\mathrm{mod}\ p)$). Действительно, символ Лежандра [9], [10] равен

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1 .$$

Соответствующее расширение поля $\mathbf{Q}$ имеет вид

$$\mathbf{Q}(i) = \left\{ z = a + bi;\ a,\ b \in \mathbf{Q},\ i^2 = -1 \right\} .$$

Тогда p-адическое нормирование продолжается на $\mathbf{Q}(i)$ с помощью функции

$$\Phi_p(z) = \sqrt{\left\| a^2 + b^2 \right\|_p} . \qquad (1.33)$$

Из неприводимости многочлена $f(t)$ $(\mathrm{mod}\ p)$ следует, что делимость целого числа $a^2 + b^2$ на p^r возможна лишь при $a,\ b \equiv 0\ (\mathrm{mod}\ p^r)$. В пополнении $\mathbf{Q}_p(i)$ поля $\mathbf{Q}(i)$ относительно нормирования (1.33) существуют первообразные корни из единицы степени N с условием $N \mid (p^2 - 1)$. В частности, для случая числа Мерсенна существуют корни степени N с условием

$$N \mid (p^2 - 1) = (p-1)(p+1) = 2^{q+1}\left(2^{q-1} - 1\right) .$$

Таким образом получаются "комплексные" варианты теоретико-числовых преобразований (в частности, для $r = 1$ хорошо известное комплексное преобразование Мерсенна [11]). Результаты вычисления свертки (1.1) получаются с точностью до "комплексного слагаемого" с целыми "действительной" и "мнимой" частями, делящимися на p^r, и при достаточно больших p и r являются точными.

1.5.4. Случай $\mathbf{Q}(\sqrt{d})$, d – вычет (mod p)

Отметим, что в этом случае вычисления в поле $\mathbf{Q}_p(\sqrt{d})$, например, с p-адической точностью $\varepsilon \le p^{-1}$ равносильны получению

вместо "истинного" результата $z = x + y\sqrt{d} \pmod p$ (заметим, что $\sqrt{d}$ есть один из элементов $1, 2, \ldots p-1$) "приближенного" результата $z_p = x_p + y_p\sqrt{d} \pmod p$, удовлетворяющего системе сравнений

$$\begin{cases} \left(x - x_p\right) + \lambda\left(y - y_p\right) \equiv 0 \pmod p \\ \left(x - x_p\right) - \lambda\left(y - y_p\right) \equiv 0 \pmod p \end{cases}, \tag{1.34}$$

следующей из определения нормирующих функций $\Psi_p^{\pm}(z) = \left\| x \pm \lambda y \right\|_p$. При $p \neq 2, d \neq 0$ система (1.34) имеет единственное решение $\left(x - x_p\right) \equiv 0 \pmod p$, $\left(y - y_p\right) \equiv 0 \pmod p$, то есть при достаточно больших p вычисления являются точными.

Кроме того, рассмотрение теоретико-числовых преобразований в поле $\mathbf{Q}_p\left(\sqrt{d}\right)$, когда d есть – вычет (mod p) позволяет в ряде случаев или снизить требования к разрядности вычислительного устройства и/или использовать для вычисления ТЧП более сложные (но и более вычислительно эффективные) редукционные схемы. Ограничимся следующим иллюстративным примером.

Пример 1.4. Пусть $f = 2^B + 1 = 2^{2b} + 1$ есть простое число Ферма. Обозначим $2^b = i$:

$$i^2 = \left(2^b\right)^2 = 2^{2b} \equiv -1 \pmod f.$$

Любой элемент поле классов вычетов $\mathbf{Z}/f\mathbf{Z}$ по модулю числа Ферма представляется в форме

$$z = z_0 + z_1 2 + \ldots + z_{b-1}2^{b-1} + 2^b\left(z_b + \ldots + z_{2b}2^b\right) =$$
$$= \left(z_0 + z_1 2 + \ldots + z_{b-1}2^{b-1}\right) + i\left(z_b + \ldots + z_{2b}2^b\right) = x + iy.$$

Распространим область "допустимых" вычислений на все кольцо

$$\left\{ z = x + iy; \quad x, y \in \mathbf{Z}/f\mathbf{Z}; \quad i^2 \equiv -1 \,(\mathrm{mod}\, f) \right\}.$$

Тогда для задачи вычисления свертки появляются дополнительные алгоритмические возможности:

- для вычисления ТЧП возможно использование аналогов БА ДПФ "по основанию четыре" и сплит-радикс БА [11], принципиально использующих тривиальность машинной реализации умножения на корни четвертой степени.

1.6. Приложения аппроксимационной теоремы

1.6.1. Параллельные алгоритмы вычисления свертки: случай неархимедово нормированных полей

Метрическая форма китайской теоремы об остатках позволяет дать также метрическое описание и алгоритмов вычисления свертки в системе остаточных классов [13].

Пусть $p_1, \ldots, p_t$ - различные простые нечетные числа; $r_1, \ldots, r_t$ - натуральные; N - таково, что в каждом из колец $\mathbf{Z}_{p_j}$ (j=1, …, t) целых p_j-адических чисел существуют первообразные корни ω_j из единицы. Пусть далее $\varepsilon = \max\limits_{1 \le j \le l} p^{-r_j}$. Определим элементы $\omega_j \in \mathbf{Z}_{p_j}$ с p_j-адической точностью ε и применим семейство дискретных преобразований (1.21) - (1.22) для вычислений приближенных значений семейства сверток $z_j(k)$ с p_j-адической точностью . Последнее означает, что "приближенное" значение $z_j(k)$ отличается от искомых "истинных" значений $z(k)$ слагаемыми,

делящимися на $p_j^{r_j}$. Тогда значения $z(k)$ могут быть реконструированы, как обычно, с помощью китайской теоремы об остатках с точностью до слагаемых, делящихся на $M = p_1^{r_1} \dots p_t^{r_t}$. Альтернативным *метрическим* подходом к реконструкции $z_j(k)$ является применение аппроксимационной теоремы утверждающей, что для заданных рациональных z_1, …, z_t существует рациональное число $\tilde{z}$, расположенное сколь угодно близко к z_j относительно семейства соответствующих p_j-адических нормирований:

$$\left|z_j - \tilde{z}\right|_{p_j} < \varepsilon \quad (j=1, 2, \dots, t). \tag{1.35}$$

При этом число $\tilde{z}$ может быть представлено в виде $\tilde{z} = z_1 b_1 + \dots + z_t b_t$ с эффективно вычислимыми рациональными b_j. Применение аппроксимационной теоремы к $z_j(k)$ определяет множество рациональных чисел $\tilde{z}(k)$, p-адические нормы которых, в силу (1.35) и целочисленности $z_j(k)$, меньше единицы. Любое такое рациональное число сравнимо $\left(\mathrm{mod}\ p_j^{r_j}\right)$ с целым числом $z(k)$, которое может быть эффективно определено. Поэтому числа $z(k)$ при достаточно большом числе $M = p_1^{r_1} \dots p_l^{r_l}$ являются точными значениями свертки (1.1).

1.6.2. Параллельные алгоритмы вычисления свертки: случай архимедово и неархимедово нормированных полей

Сформулированная выше аппроксимационная теорема остается справедливой и в случае, когда одно из нормирований архимедово. Это позволяет решить следующую задачу.

Задача. *Пусть в распоряжении пользователя имеется два процессора:*

(а) реализующий (приближенное) вычисление целочисленной свертки (1.1) *с помощью комплексного ДПФ с гарантированной абсолютной погрешностью, не превосходящей* ε_∞;

(б) реализующий вычисление свертки (1.1) *в арифметике* $(\mathrm{mod}\ p)$ *с p-адической погрешностью, не превосходящей* ε_p, *причем для простого числа p не выполняется неравенство* (1.4), *то есть простое число p "недостаточно велико".*

Можно ли при этих условиях, располагая дополнительной априорной информацией о точности вычислений ε_∞, *вычислить свертку* (1.1) ***точно****?*

Пусть при вычислении свертки (1.1) целочисленных вещественных последовательностей с помощью комплексного ДПФ получаются приближенные результаты, которые будем считать вещественными рациональными числами $z_\infty(k)$, отличающиеся от истинных значений $z(k)$:

$$\left|z(k)-z_\infty(k)\right|<\varepsilon<\varepsilon_\infty. \tag{1.36}$$

Применение ТЧП $(\mathrm{mod}\ p)$ в $\mathbf{Q}_p$ дает в качестве результатов целые числа $z_p(k)$ с погрешностью, оцениваемой в p-адической метрике:

$$\left|z(k)-z_p(k)\right|_p<\varepsilon_p=p^{-1}. \tag{1.37}$$

Сравнивая (1.36) и (1.37), получаем соотношения

$$z_\infty(k)-\varepsilon<z(k)<z_\infty(k)+\varepsilon;\quad z(k)=z_p(k)+ps,\quad s=0,\pm1,\pm2\ldots,$$

Но в интервале $\left(z_\infty(k)-\varepsilon, z_\infty(k)+\varepsilon\right)$ при $p>2\varepsilon$ может бы только одно целое число вида $z_p(k)+ps$, которое и является искомым значением $z(k)$. В неформальных терминах: вычисления с помощью ДПФ "точны в старших разрядах результата", а вычисления с помощью ТЧП "точны в младших разрядах результата". Сравнение найденных массивов $z_\infty(k)$, $z_p(k)$ и применение аппроксимационной теоремы дают возможностью найти точные значения $z(k)$ параллельным вычислением (1.1) с помощью ДПФ и ТЧП по относительно небольшому модулю, выбор которого определяется предполагаемой погрешностью вычисления ДПФ.

ЧАСТЬ 2. НЕОДНОЗНАЧНОСТЬ РАЗЛОЖЕНИЯ НА МНОЖИТЕЛИ И ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЯ СВЕРТКИ

Оказывается, среди математиков существует глубоко укоренившаяся тенденция предполагать единственность разложения на простые. Эта тенденция, несомненно, навеяна опытом вычислений с обычными целыми числами <…>. Свидетельством силы этой тенденции служит использование Эйлером в его "Алгебре" единственности разложения для квадратичных целых, несмотря на контрпример

$$3 \cdot 7 = \left(4 + \sqrt{-5}\right)\left(4 - \sqrt{-5}\right),$$

известный как ему, так и за сто лет до него Пьеру Ферма.

Г.Эдвардс[1].

2.1. Введение, основные идеи

Как уже отмечалось в предыдущей части наиболее существенным недостатком теоретико-числовых преобразований (ТЧП)

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\omega^{mn} \pmod{p},\ \omega^N \equiv 1 \pmod{p} \qquad (2.1)$$

является то, что простые числа p с "дружественными" для машинной реализации свойствами модулярных операций (простые числа

---

[1] Г.Эдвардс. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел.* М.:Мир, 1980.

Мерсенна, Ферма, Голомба и т.п.) встречаются в натуральном ряду достаточно редко. Кроме того, в отличие от поля комплексных чисел, в конечном поле $\mathbf{GF}(p)$ существуют корни не любой степени N из единицы, а только удовлетворяющие условию делимости:

$$N \left| (p-1) \right. . \qquad (2.2)$$

Для чисел Ферма

$$f_t = 2^B + 1, \; B = 2^t \qquad (2.3)$$

это стеснительное, в общем случае, ограничение (2.2) гарантирует существование структурно простых быстрых алгоритмов вычисления преобразования (2.1) длины, равной степени двойки. С другой стороны, наиболее просто реализуется преобразование (2.1) при $\omega \equiv 2 \pmod{f_t}$. В этом случае умножения на фазовые множители в модулярной версии алгоритма Кули-Тьюки (БПФ) реализуются без нетривиальных вещественных умножений. К сожалению, в силу соотношения (2.3), элемент $\omega \equiv 2 \pmod{f_t}$ является корнем степени $N = 2B$ в поле $\mathbf{GF}(f_t)$, что ограничивает максимальную длину преобразования Ферма, реализуемого без умножений, числом $N = 32$.

Кроме того, для "безошибочного" вычисления свертки спектральным методом с использованием ТЧП число p должно быть достаточно велико. В частности, при решении достаточно типичной для цифровой обработки изображений задачи вычисления двумерной свертки двух целочисленных массивов размера (512×512) с диапазонами изменения значений $0 \div 255$, для числа $p = f_t$ должно выполняться неравенство:

$$p > (512)^2 \; (256)^2 = 2^{34} > f_4 = 2^{16} + 1.$$

Это существенно ограничивает возможности применения ТЧП Ферма в задачах обработки многомерной цифровой информации.

Использование в качестве модулей в преобразовании (2.1) составных чисел Ферма доставляет серьезные трудности, связанные с существованием в модулярных кольцах по составным модулям делителей нуля и, как следствие, с необратимостью некоторых элементов соответствующих колец и/или с неортогональностью базисных функций преобразования (2.1).

Действительно, доказательство ортогональности базисных функций дискретного преобразования Фурье длины N сводится к проверке равенства

$$\sum_{n=0}^{N-1} \omega^{mn} \omega^{-nk} = \begin{cases} \dfrac{1-\omega^{N(m-k)}}{1-\omega^{(m-k)}} = 0, & \text{при } m \neq k \ (\mathrm{mod}\, N); \\ N, & \text{при } m \equiv k \ (\mathrm{mod}\, N). \end{cases} \qquad (2.4)$$

Доказательство последнего соотношения представляет собой тривиальное упражнение на суммирование геометрической прогрессии и остается справедливым и для случая конечного поля, в котором существует корень степени N из единицы. Условие "быть полем", то есть простота модуля в (2.1), существенна. В поле только нулевой элемент необратим, что гарантирует возможность "деления" на элемент $\left(1-\omega^{(m-k)}\right)$ в верхней строчке правой части равенства (2.4).

При составном модуле элемент $\left(1-\omega^{(m-k)}\right)$ в соотношении (2.4) может быть необратимым и для несравнимых по $\left(\mathrm{mod}\, N\right)$ значений m,k. При распараллеливании вычислений в системе остаточных классов характерные преимущества "битовой" реализации арифметических операций в полях по модулям чисел Мерсенна и Ферма не наследуются для вычислений в полях по модулям целых делителей составных чисел Мерсенна или Ферма

$$m = 2^q \pm 1 = p_1 p_2 \ldots p_d \qquad (2.5)$$

В самом деле, например, для пятого числа Ферма справедливо разложение на простые сомножители $f_5 = 2^{32} + 1 = 641 \times 6700417$. Эти сомножители уже не являются числами Ферма. Вышесказанное относится в значительной степени и к составным числам Мерсенна.

<u>Основные идеи</u>: давайте, во-первых, попробуем представить сомножители правой части соотношения (2.5) в "фермаподобной" или "мерсенноподобной" формах, выбирая для этих сомножителей такие подходящие элементы $\alpha_j^{k_j}$ кольца $\mathbf{Z}/m\mathbf{Z}$, чтобы сомножители в (2.5) имели вид $p_j = \alpha_j^{k_j} \pm 1$, причем операции в кольцах $\mathbf{Z}/p_j\mathbf{Z}$ для элементов, представленных в "системе счисления с основаниями $\alpha_j^{k_j}$, реализовывались бы достаточно просто. Во-вторых, если таких "хороших" элементов $\alpha_j^{k_j}$ в кольце $\mathbf{Z}/m\mathbf{Z}$ найти не удается, то рассмотрим расширение кольца $\mathbf{Z}/m\mathbf{Z}$ и попытаемся найти такие "хорошие" элементы $\alpha_j^{k_j}$ в расширении, используя возможную неоднозначность разложения элементов в кольцах целых элементов полей алгебраических чисел. В первом случае получается альтернативное представление сомножителей в (2.5), во втором – альтернативное разложение (2.5) в некотором бóльшем кольце.

Таким образом, целью данной части пособия является рассмотрение методов вычисления дискретной свертки с помощью дискретных преобразований, реализуемых без умножений, ориентированных на представление данных в "нетрадиционных" системах

счисления и сохраняющих преимущества арифметики Мерсенна или Ферма и для составных чисел указанного вида.

В основе предложенных методов лежит следующая схема вычислений.

1. Кольцо классов вычетов $\mathbf{Z}/m\mathbf{Z}$ по, вообще говоря, составному модулю m вкладывается в некоторое кольцо $\mathbf{W}$, которое в ряде случаев является алгебраическим расширением кольца классов вычетов $\mathbf{Z}/m\mathbf{Z}$.

2. Кольцо $\mathbf{W}$ выбирается так, чтобы разложение (2.5) на простые элементы кольца $\mathbf{W}$ содержало только сомножители вида $p_j = \alpha_j^{k_j} \pm 1$.

3. Вычисление свертки проводится по обычной параллельной схеме с применением семейства некоторых дискретных преобразований (аналогов ТЧП) в системе остаточных классов $(\mathrm{mod}\ p_j)$ с последующей реконструкцией значения свертки $(\mathrm{mod}\ m)$ по китайской теореме об остатках.

4. Базисные функции $h_m^j(n)$ семейства этих преобразований выбираются в форме $h_m^j(n) = \alpha_j^{nm}$; если входные данные преобразований $(\mathrm{mod}\ p_j)$ представлены в позиционной системе счисления "с основанием α_j", то вычисление ТЧП, как и, например, в мерсенновском случае, не требует умножений.

Эффективность реализации предложенной схемы вычислений связана, естественно, с возможностью эффективной реализации вычислений при представлении данных в "нетрадиционных" системах счисления.

Отметим также, что рассматриваемые параллельные алгоритмы, использующие "альтернативное" разложение целых чисел в кольце $\mathbf{W}$, переходят в "обычные" алгоритмы вычисления свертки с помощью ТЧП Мерсенна и/или Ферма в случае простоты этих чисел, то есть в случаях, когда в кольце целых чисел нет нетривиального разложения модулей на множители.

2.2. Параллельные алгоритмы вычисления свертки по модулю составного числа Мерсенна

2.2.1. Альтернативное представление разложения (составных) чисел Мерсенна

Определение 2.1. Пусть $q = 2^{2t+1} - 1$ есть (составное) число Мерсенна, такое что:

- при всех $1 < s < 2t+1$ числа q и $2^s - 1$ взаимно просты:

$$\text{н.о.д.}\left(q,\ 2^s - 1\right) = 1; \tag{2.6}$$

- элемент $2t+1$ обратим в кольце $\mathbf{Z}/q\mathbf{Z}$.

Такие числа Мерсенна будем называть *нормальными числами Мерсенна*.

Рассмотрим кольцо $\mathbf{S}\left(\sqrt{2}\right) = \mathbf{S}$ целых элементов поля $\mathbf{Q}\left(\sqrt{2}\right)$, то есть таких элементов $z = a + b\sqrt{2} \in \mathbf{Q}\left(\sqrt{2}\right)$, что при $d = 2$ *норма и след* есть целые числа:

$$\mathbf{Norm}(z) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2 \in \mathbf{Z},$$
$$\mathbf{Tr}(z) = \left(a + b\sqrt{d}\right) + \left(a - b\sqrt{d}\right) = 2a \in \mathbf{Z}.$$

В кольце $\mathbf{S}$ для числа q наряду с представлением в виде произведения целых рациональных чисел ("обычных" целых чисел) возможно представление в форме

$$q=\left(2^t\sqrt{2}+1\right)\left(2^t\sqrt{2}-1\right). \qquad (2.7)$$

Лемма 2.1. *Элементы* $q_1,\ q_2\in\mathbf{S}$

$q_1=2^t\sqrt{2}+1$ *и* $q_2=2^t\sqrt{2}-1$

взаимно просты в $\mathbf{S}$.

Доказательство. Допустим противное: пусть существуют $a,\ b_1,\ b_2\in\mathbf{S}$, не являющиеся единицами в $\mathbf{Q}\left(\sqrt{2}\right)$, такие что $q_1=ab_1$, $q_2=ab_2$. Так как норма $\mathbf{Norm}(z)$ элемента $z=x+y\sqrt{2}\in\mathbf{Q}\left(\sqrt{2}\right)$ равна $\mathbf{Norm}(z)=x^2+2y^2$ и является мультипликативной функцией: $\mathbf{Norm}(wz)=\mathbf{Norm}(w)\cdot\mathbf{Norm}(z)$, то из очевидных равенств

$q_1=q_2+2$, $a(b_1-b_2)=2$

следует

$$4=\mathbf{Norm}(2)=\mathbf{Norm}\left(a(b_1-b_2)\right)=\mathbf{Norm}(a)\mathbf{Norm}(b_1-b_2).$$

Следовательно, $\mathbf{Norm}(a)$ является четным числом, что противоречит равенству

$$\mathbf{Norm}(q_1)=\mathbf{Norm}(ab_1)=q=2^{2t+1}-1=\mathbf{Norm}(a_1)\cdot\mathbf{Norm}(b_1).$$

Из Леммы 2.1 следует, в частности, что кольцо $\mathbf{z}/q\mathbf{z}$ изоморфно вкладывается в прямую сумму $\mathbf{S}_1\oplus\mathbf{S}_2$, где $\mathbf{S}_1$ и $\mathbf{S}_2$ - кольца клас-

сов вычетов кольца $\mathbf{S}$ по главным идеалам, порожденным элементами q_1 и q_2 соответственно.

Наличие представления (2.7) и Лемма 2.1 позволяют свести вычисление целочисленной свертки в арифметике кольца $\mathbf{Z}/q\mathbf{Z}$ к параллельному вычислению двух сверток в кольцах $\mathbf{S}_1$, $\mathbf{S}_2$ и последующей реконструкции результата с помощью стандартного применения китайской теоремы об остатках.

Замечание 2.1. Отметим, что для чисел Мерсенна сравнение $z^2 \equiv 2 \pmod{q}$ имеет решения в кольце $\mathbf{Z}/q\mathbf{Z}$, то есть $\pm\sqrt{2} \in \mathbf{Z}/q\mathbf{Z}$. Действительно,

$$\left(\pm 2^{t+1}\right)^2 \equiv 2 \cdot 2^{2t+1} \equiv 2 \left(\mathrm{mod}\left(2^{2t+1} - 1\right)\right), \qquad (2.8)$$

поэтому более корректно говорить об *альтернативном представлении разложения* (составного) числа Мерсенна на взаимно простые сомножители. Действительно, если число Мерсенна простое, то сравнение $z^2 \equiv 2 \pmod{q}$ имеет ровно два решения, равные $z_{1,2} = \pm 2^{t+1}$. В этом случае $\left(2^t\sqrt{2} - 1\right) = q \equiv 0 \,(\mathrm{mod}\, q)$. Если число Мерсенна составное, то сравнение $z^2 \equiv 2 \pmod{q}$ может иметь больше, чем два решения. Множество этих решений разбивается на пары, элементы которых противоположны по знаку. Каждой паре этих решений соответствует разложение модуля на два взаимно простых множителя, причем некоторые разложения оказываются тривиальными (один из сомножителей сравним с $\pm 1 \pmod{q}$). Подробнее этот вопрос рассматривается в конце раздела в Примере 2.1.

Вместо арифметики кольца вычетов $(\mathrm{mod}\ q)$ удобнее рассматривать арифметику изоморфного кольца $(\mathrm{mod}\ (-q))$. Тогда

$$(-q)=\left(2^t\left(-\sqrt{2}\right)-1\right)\left(2^t\sqrt{2}-1\right)=\left(\left(-\sqrt{2}\right)^{2t+1}-1\right)\left(\left(\sqrt{2}\right)^{2t+1}-1\right).$$

Положим:

$$(-q)=Q,\ P=\left(\left(\sqrt{2}\right)^{2t+1}-1\right),\ R=\left(\left(-\sqrt{2}\right)^{2t+1}-1\right),\alpha=\sqrt{2}\ ,\ \beta=-\sqrt{2}\ ;$$

символами (P) и (R) обозначим главные идеалы, порожденные элементами P и R соответственно.

Лемма 2.2. *Для любого* $X=\mathbf{z}/_{Q\mathbf{z}}$ *существуют эффективно определяемые элементы* $Y,\ Z\in \mathbf{S}/_{(Q)}$ *и константы* $a,\ b\in \mathbf{z}/_{Q\mathbf{z}}$ *такие, что:*

(a) справедливо равенство

$$X=aYP+bZR, \tag{2.9}$$

причем

$$X\equiv Y\left(\mathrm{mod}\ \ (R)\right),\ X\equiv Z\left(\mathrm{mod}\ \ (P)\right);$$

(b) Y и Z представляются в форме:

$$Y=A_1+A_2\sqrt{2}\ ,Z=B_1+B_2\sqrt{2}\ ,0\le A_1,\ B_1<2^{t+1},0\le A_2,\ B_2<2^t\ .$$

Доказательство. Так как по Лемме 2.1 идеалы (P) и (R) взаимно просты, то утверждение (a) леммы 2.2 является следствием китайской теоремы об остатках.

Положим $a=b=-2^{-1}(\mathrm{mod}Q)$, что корректно в силу обратимости элемента $2\left(\mathrm{mod}\ \ Q\right)$. Тогда

$$X=a\ \ \left(B_1+B_2\left(-\sqrt{2}\right)\right)\left(\left(\sqrt{2}\right)^{2t+1}-1\right)+b\left(A_1+A_2\sqrt{2}\right)\left(\left(-\sqrt{2}\right)^{2t+1}-1\right),$$

откуда следует система сравнений для определения A_1 , B_1 :

$$\begin{cases} 2^t\left(a\ \ B_1-b\ \ A_1\right)-\left(b\ \ A_2-aB_2\right)\equiv 0\ \ \left(\mathrm{mod}\ \ Q\right), \\ -2^{t+1}\left(a\ \ B_2+b\ \ A_2\right)-\left(a\ \ B_1+b\ \ A_1\right)\equiv X\ \ \left(\mathrm{mod}\ \ Q\right)\ . \end{cases} \tag{2.10}$$

Далее, умножая первое уравнение системы на 2^{t+1} и учитывая, что $2^{2t+1} = 1(\mathrm{mod}\, Q)$, получим эквивалентную систему

$$\begin{cases} A_1 + 2^{t+1} A_2 \equiv X(\mathrm{mod}\, Q), \\ B_1 + 2^{t+1} B_2 \equiv X(\mathrm{mod}\, Q). \end{cases}$$

Покажем, что среди решений последней системы сравнений существуют решения с условиями:

$0 \le A_1,\ B_1 < 2^{t+1},\ 0 \le A_2,\ B_2 < 2^t$.

Действительно, пусть χ - наименьший неотрицательный вычет X по модулю Q, **quot**$(u // v)$ - неполное частное деления u на v. Тогда

$$\begin{cases} A_2 = B_2 = \mathbf{quot}(\chi // 2^{t+1}), \\ A_1 = B_1 = \chi - 2^{t+1} A_2 \ . \end{cases}$$

Элементы A_1, B_1 требуют для представления двоичным кодом $(t+1)$ бит, элементы A_2, B_2 допускают t-битовое представление. Пусть $a_j^i = 0,\ 1$ и

$$A_1 = 2^t a_t^1 + 2^{t-1} a_{t-1}^1 + \ldots + 2^0 a_0^1;$$

$$A_2 = 2^{t-1} a_{t-1}^2 + \ldots + 2^0 a_0^2 . \qquad (2.11)$$

Тогда, с учетом обозначений (2.9), имеем $(2t+1)$- битовое представление для Z "в системе счисления с иррациональным основанием $\alpha = \sqrt{2}$ ":

$$Z = \alpha^{2t} a_t^1 + \alpha^{2t-1} a_{t-1}^2 + \alpha^{2t-2} a_{t-1}^1 + \ldots + \alpha^1 a_0^2 + \alpha^0 a_0^1 . \qquad (2.12)$$

Аналогично, элемент Y представим "в системе счисления с основанием $\beta = -\sqrt{2}$ ":

$$Y = \beta^{2t} b_t^1 + \beta^{2t-1} \beta_{t-1}^2 + \beta^{2t-2} b_{t-1}^1 + \ldots + \beta^1 b_0^2 + \beta^0 b_0^1 , \qquad (2.13)$$

что и доказывает утверждение (б) леммы. ♦

Далее элементы A_1 и A_2 для элемента Z, представленного в форме (2.12), будем называть рациональной и иррациональной частями для Z и обозначать:

$$A_1 = \mathbf{Rat}(Z),\ A_2 = \mathbf{Irr}(Z);\ Z = \mathbf{Rat}(Z) + \sqrt{2}\,\mathbf{Irr}(Z).$$

Как обычно, представление X в форме (2.9) ассоциируется с разложением кольца вычетов $(\mathrm{mod}\ q)$ в прямую сумму колец. Поэтому, с точностью до проектирующего мономорфизма, можно считать, что $Z \in \mathbf{S}_1$, $Y \in \mathbf{S}_2$. Умножение элемента Z приводит к левому циклическому сдвигу "цифр" a_j^i в (2.24). Умножение элементов A_1 и A_2 на 2 приводит к левому циклическому сдвигу "цифр" a_j^1 и a_j^2 в (2.23). Умножение элементов Z_1 и Z_2, представленных в форме (2.23) в силу равенства

$$\begin{aligned}&\mathbf{Rat}(Y_1Y_2) + \sqrt{2}\mathbf{Irr}(Y_1Y_2) = \left(\mathbf{Rat}(Y_1)\mathbf{Rat}(Y_2) + 2\mathbf{Irr}(Y_1)\mathbf{Irr}(Y_2)\right) + \\ &+\sqrt{2}\left(\mathbf{Rat}(Y_1)\mathbf{Irr}(Y_2) + \mathbf{Rat}(Y_2)\mathbf{Irr}(Y_1)\right),\end{aligned} \tag{2.14}$$

сводится к известной "битовой" интерпретации мерсенновской арифметики. Аналогичные соотношения справедливы и в кольце $\mathbf{S}_2$. Сложение элементов в форме (2.12) также реализуется по правилам, близким к мерсенновским: двоичное сложение с переносами в старшие разряды по правилам $2\alpha^j = \alpha^{j+2}$, $\alpha^j = \alpha^{2t+1} = \alpha^0$.

Лемма 2.2. *Если* $q = 2^{2t+1} - 1$ *является нормальным числом Мерсенна, то функции* $h_m^{\alpha}(n) = \alpha^{mn} \in \mathbf{S}_1$ *и* $h_m^{\beta}(n) = \beta^{mn} \in \mathbf{S}_2$ *образуют ортогональные семейства*:

$$\left\langle h_m^{\gamma},\ h_k^{\gamma} \right\rangle = \sum_{n=0}^{q-1} h_m^{\gamma}(n)\ h_k^{\gamma}(q-n) = q \cdot \delta_{mk}\ (\gamma = \alpha,\ \beta).$$

Доказательство. Так как $\alpha^q = 1 \in \mathbf{S}_1$, $\beta^q = 1 \in \mathbf{S}_2$, то единственной причиной нарушения условия ортогональности может быть необратимость элементов $\left(1-\alpha^{m-k}\right)$ и $\left(1-\beta^{m-k}\right)$ при суммировании геометрических прогрессий, что влечет существование общего делителя чисел $\left(1-\left(\sqrt{2}\right)^{m-k}\right)\left(1-\left(-\sqrt{2}\right)^{m-k}\right)$ и q. Это невозможно в силу нормальности рассматриваемого числа Мерсенна. Действительно, если $m > k, (m-k) > 2$, то

$$\left(1-\left(\sqrt{2}\right)^{m-k}\right)\left(1-\left(-\sqrt{2}\right)^{m-k}\right) = \begin{cases} \left(1-\left(\sqrt{2}\right)^{m-k}\right)^2, \text{если } (m-k) \equiv 0 \pmod 2 \\ \left(1-2^{m-k}\right), \text{если } (m-k) \neq 0 \pmod 2 \end{cases}.$$

Если $0 < (m-k) \le 2$, то

$$\left(1-\left(\sqrt{2}\right)^{m-k}\right)\left(1-\left(-\sqrt{2}\right)^{m-k}\right) \equiv \begin{cases} -1 \pmod q & \text{при } (m-k) = 1; \\ +1 \pmod q & \text{при } (m-k) = 2, \end{cases}$$

откуда следует обратимость элементов $\left(1-\left(\pm\sqrt{2}\right)^{m-k}\right)$ в кольцах $\mathbf{S}_1$ и $\mathbf{S}_2$. ♦

2.2.2. Вычисление свертки по модулю составного числа Мерсенна

Пусть $\mathbf{J}$ есть один из идеалов (P) или (R). Введем оператор (левого) сдвига Мерсенна, определенный на множестве редуцированных $(\mathrm{mod}\,\mathbf{J})$ двоичных кодов

$$\langle X_T,\ X_{T-1},\ \ldots,\ X_0 \rangle = \langle X \rangle_{\mathbf{J}}. \qquad (2.15)$$

посредством равенства ("перенос переполняющей компоненты X_T в младший разряд"):

$$\mathrm{M}\ \langle X\rangle_{\mathbf{J}} = \langle X_{T-1},\ \ldots,\ X_0,\ X_T\rangle. \qquad (2.16)$$

Аналогично определялся обратный оператор (правого) сдвига Мерсенна:

$$\mathrm{M}^{-1}\langle X\rangle_{\mathbf{J}} = \langle X_0,\ X_T,\ X_{T-1},\ \ldots,\ X_1\rangle. \qquad (2.17)$$

Определение 2.2. Пусть $x(n)$ есть T-периодическая последовательность элементов кольца $\mathbf{S}_1$ или $\mathbf{S}_2$; $\mathbf{J}$ есть один из идеалов (P) или (R); $T = 2t+1$; Определим *шифт-преобразование Мерсенна* последовательности $x(n)$ равенствами:

$$\langle X_k(m)\rangle = \sum_{n=0}^{T-1} \mathrm{M}^{mn}\langle x(n)\rangle_{\mathbf{J}} \quad (m = 0,\ 1,\ \ldots,\ T-1), \qquad (2.18)$$

где k = 1,2 в зависимости от того, какое из колец рассматривается: $\mathbf{S}_1$ или $\mathbf{S}_2$.

Так как действие оператора левого мерсенновского сдвига кода равносильно умножению числа, представленного этим кодом на элемент $2(\mathrm{mod}\ \mathbf{J})$, то нетрудно показать, что имеет место равенство

$$\langle T\cdot x(n)\rangle_{\mathbf{J}} = \sum_{m=0}^{T-1} \mathrm{M}^{-mn}\ \langle X_k(m)\rangle_{\mathbf{J}}. \qquad (2.19)$$

Рассмотренные выше преобразования сдвига кодов (*шифт-преобразования*) позволяют вычислять циклическую свертку целочисленных T-периодических последовательностей с помощью "T – битовых мерсенновских процессоров" по обычной спектральной схеме. Алгоритм вычисления свертки с помощью шифт-ТЧП структурно аналогичен хорошо известному алгоритму параллельного вычисления свертки в системе остаточных классов.

Теорема 2.1. *Если выполняются условия Леммы 2.2 и для преобразуемой последовательности* $x(n)$ *с помощью метода леммы 2.2 найдены проекции* $y(n)$ *и* $z(n)$ *в кольца* $\mathbf{S}_1$ *и* $\mathbf{S}_2$, *то для вычисления свертки (2.1) длины* $T = 2t+1$ *достаточно выполнения:*

- *шести шифт-ТЧП Мерсенна (четырех прямых и двух обратных);*
- *вычисления произведений компонент спектров шифт-ТЧП в "традиционной" мерсенновской арифметике;*
- *реконструкции значений свертки по китайской теореме об остатках.*

Доказательство. Два последних шага традиционны; обоснование первого шага следует из интерпретации действия оператора M на битовый вектор

$$\left(a_t^1,\ a_{t-1}^2,\ a_{t-1}^1,\ \ldots,\ a_0^2,\ a_0^1\right)$$

как умножения на элемент $\alpha = \sqrt{2}$ элемента

$$\alpha^{2t}a_t^1 + \alpha^{2t-1}a_{t-1}^2 + \alpha^{2t-2}a_{t-1}^1 + \ldots + \alpha^1 a_0^2 + \alpha^0 a_0^1 .$$ ♦

В таблице 2.1. приведены разложения чисел $\left(2^s - 1\right) = q$ на простые сомножители. Эти численные данные дают основания утверждать, что числа Мерсенна, в том числе и составные, являются нормальными для всех простых s, по крайней мере, в диапазоне $2 \le s \le 53$ (в таблице индексы нормальных чисел выделены).

Пример 2.1. Вернемся к замечанию 2.1. Рассмотрим $q = q_{11} = 2^{11} - 1 = 2047 = 23 \times 89$. Сравнение $\alpha^2 \equiv 2 \pmod q$ имеет четыре решения:

$$\alpha_1 \equiv 2^{5+1} \equiv 64 \pmod{2047}, \quad \alpha_2 \equiv -2^{5+1} \equiv 983 \pmod{2047},$$
$$\alpha_3 \equiv 915 \pmod{2047}, \quad \alpha_4 \equiv 1132 \pmod{2047}.$$

Приведем явные численные выражения для $\left(2^{t}\sqrt{2}+1\right)\left(2^{t}\sqrt{2}-1\right)$, полагая $\sqrt{2}\equiv\alpha_j \pmod{2047}$, $j=1,2,3,4$.

$$\left(2^5\alpha_1+1\right)\left(2^5\alpha_1-1\right)\equiv\left(2^5 2^6+1\right)\left(2^5 2^6-1\right)\equiv$$
$$\equiv 2049\times 2047 \pmod{2047}\equiv 2\times 2047 \pmod{2047},$$
$$\left(2^5\alpha_2+1\right)\left(2^5\alpha_2-1\right)\equiv\left(2^5(-2^6)+1\right)\left(2^5(-2^6)-1\right)\equiv$$
$$\equiv(-2047)\times(-2049) \pmod{2047}\equiv(-2047)\times(-2) \pmod{2047},$$
$$\left(2^5\alpha_3+1\right)\left(2^5\alpha_3-1\right)\equiv 29281\times 29279\equiv(329\times\mathbf{89})\times(1273\times\mathbf{23}) \pmod{2047},$$
$$\left(2^5\alpha_4+1\right)\left(2^5\alpha_4-1\right)\equiv 36225\times 36223\equiv\left(3^2 5^2 7\times\mathbf{23}\right)\times\left(407\times\mathbf{89}\right) \pmod{2047}.$$

Таким образом, представление целого числа w, например в кольце классов вычетов $\mathrm{mod}\left(2^5\alpha_3-1\right)$, выглядит следующим образом:

$$w\equiv w_0 915^0+0\cdot 915^1+w_1 915^2+0\cdot 915^3+\ldots+w_{k(w)}915^{2k(w)}\equiv$$
$$\equiv w_0 2^0+0\cdot 915^1+w_1 2^1+0\cdot 915^3+\ldots+w_{k(w)}2^{k(w)} \left(\mathrm{mod}\left(2^5\alpha_3-1\right)\right),$$

где w_j - цифры обычного представления числа w в двоичной системе счисления

$$w=w_0 2^0+w_1 2^1+\ldots+w_{k(w)}2^{k(w)}.$$

Таблица 2.1

Факторизация чисел Мерсенна $q_s = 2^s - 1 \left(2 \le s \le 53\right)$

s	**Факторизация**	s	**Факторизация**
2	3	28	$3\times5\times29\times43\times113\times127$
3	7	**29**	$233\times1103\times2089$
4	3×5	30	$3^2 7\times11\times31\times151\times331$
5	31	**31**	2147483647
6	$3^2 7$	32	$3\times5\times17\times257\times65537$
7	127	33	$7\times23\times89\times599479$
8	$3\times5\times17$	34	$3\times43691\times131071$
9	7×73	35	$31\times71\times127\times122921$
10	$3\times11\times31$	36	$3^3 5\times7\times13\times19\times37\times73\times109$
11	23×89	**37**	223×616318177
12	$3^2 5\times7\times13$	38	$3\times174763\times524287$
13	8191	39	$7\times79\times8191\times121369$
14	$3\times43\times127$	40	$3\times5^2 11\times17\times31\times41\times61681$
15	$7\times31\times151$	**41**	13367×164511353
16	$3\times5\times17\times257$	42	$3^2 7^2 43\times127\times337\times5419$
17	131071	**43**	$431\times9719\times2099863$
18	$3^3 7\times19\times73$	44	$3\times5\times23\times89\times397\times683\times2113$
19	524287	45	$7\times31\times73\times151\times631\times23311$
20	$3\times5^2 11\times31\times41$	46	$3\times47\times178481\times2796203$
21	$7^2 127\times337$	**47**	$2351\times4513\times13264529$
22	$3\times23\times89\times683$	48	$3^2 5\times7\times13\times17\times97\times241\times257\times673$
23	47×178481	49	$127\times443\times2676798593$
24	$3^2 5\times7\times13\times17\times241$	50	$3\times11\times31\times251\times601\times1801\times4051$
25	$31\times601\times1801$	51	$7\times103\times2143\times11119\times131071$
26	$3\times2731\times8191$	52	$3\times5\times53\times157\times1613\times2731\times8191$
27	$7\times73\times262657$	**53**	$6361\times69431\times20394401$

2.3. Параллельные алгоритмы вычисления свертки по модулю составного числа Ферма

2.3.1. Альтернативное разложение (составных) чисел Ферма

В предыдущем разделе рассматривался алгоритм вычисления свертки, основанный на альтернативном представлении разложения составных чисел Мерсенна на множители. В настоящем разделе рассматривается алгоритм вычисления свертки, основанный на альтернативном разложении составных чисел Ферма в кольце целых некоторого кубического поля алгебраических чисел. Если $f = 2^B + 1 \left(B = 2^s\right)$ есть число Ферма, то кольцо $\mathbf{Z}/_{(f)}$ не содержит корней третьей степени из единицы. В этом случае желаемый эффект достигается при использовании кубических расширений поля $\mathbf{Q}$. Следует отметить, что основную техническую трудность представляет отыскание явного вида вложения кольца вычетов $\mathbf{Z}/_{(f)}$ в прямую сумму колец. Доказательство Леммы 2.4, гарантирующей взаимную простоту сомножителей альтернативного разложения чисел Ферма, может быть пропущено при первом чтении без ущерба для понимания дальнейшего.

Определение 2.3. *Нормальным числом Ферма* будем называть число Ферма f с условиями:

- при всех $1 < s < 3t + 1$ числа f и $2^s - 1$ взаимно просты;
- элемент $2(3t+1)$ обратим в фактор-кольце $\mathbf{Z}/_{(f)}$;
- число f не делится на 3, то есть $f \neq 0 \pmod 3$.

Пусть теперь, для определенности, нормальное число Ферма f имеет вид

$$f = 2^B + 1,\ B = 2^s = 3t + 1. \qquad (2.20)$$

Пусть $\mathbf{S}$ – кольцо целых элементов поля $\mathbf{F}$ разложения полинома $\varphi(z) = z^3 + 2$ над $\mathbf{Q}$. В кольце $\mathbf{S} \supseteq \mathbf{Z}$ для числа f, наряду с обычным представлением составного числа в виде произведения целых рациональных чисел, возможно представление в форме

$$f = \left(2^t \sqrt[3]{2} + 1\right)\left(2^t \gamma \sqrt[3]{2} + 1\right)\left(2^t \overline{\gamma} \sqrt[3]{2} + 1\right), \qquad (2.21)$$

где γ - примитивный корень третьей степени из единицы.

Лемма 2.4. *Элементы* $f_1, f_2, f_3 \in \mathbf{S}$ *:*

$$f_1 = \left(2^t \sqrt[3]{2} + 1\right),\ f_2 = \left(2^t \gamma \sqrt[3]{2} + 1\right),\ f_3 = \left(2^t \overline{\gamma} \sqrt[3]{2} + 1\right)$$

попарно взаимно просты в кольце $\mathbf{S}$**.**

Доказательство. Допустим, что существуют $a, b_1, b_2 \in \mathbf{S}$, не являющиеся единицами кольца $\mathbf{S}$ такие, что $f_1 = a\, b_1, f_2 = a\, b_2$. Нормальным полем для многочлена $\varphi(z)$ является поле $\mathbf{F} = \mathbf{Q}\left(\gamma, \sqrt[3]{2}\right)$. Пусть $\mathbf{Norm}_\gamma(x)$ есть относительная норма элемента $x \in \mathbf{F}$ в поле $\mathbf{Q}(\gamma)$. Трехэлементная группа Галуа полинома $\varphi(z)$ над подполем $\mathbf{Q}(\gamma)$ циклична и действует тождественно на $\mathbf{Q}$. Относительная норма элемента $z = x + y\sqrt[3]{2} \in \mathbf{S}$ равна $\mathbf{Norm}_\gamma(x) = x^3 + 2y^3$. Поэтому из очевидных равенств

$$f_2 = \gamma f_1 + 1 - \gamma,\ f_2 - f_1 = (f_1 - 1)(\gamma - 1)$$

следует

$$\mathbf{Norm}_\gamma(f_1 - 1)\ \mathbf{Norm}_\gamma(\gamma - 1) = \mathbf{Norm}_\gamma(a)\ \mathbf{Norm}_\gamma(a),$$

$$2^B(\gamma - 1)^3 = \mathbf{Norm}_\gamma(a)\ \mathbf{Norm}_\gamma(a). \qquad (2.22)$$

Так как $\mathbf{Norm}_\gamma(a)$ не может быть четным числом, что противоречило бы равенству

$$\mathbf{Norm}_{\gamma}(f_1) = \mathbf{Norm}_{\gamma}(ab_1) = f = 2^B + 1 = \mathbf{Norm}_{\gamma}(a)\ \mathbf{Norm}_{\gamma}(b_1),$$

то равенство (2.22) может выполняться только при условии делимости

$$\mathbf{Norm}_{\gamma}(a) \mid (\gamma - 1)^3. \qquad (2.23)$$

Так как $\mathbf{Norm}_{\gamma}(a) \in \mathbf{Q}(\gamma)$, то, вычисляя норму элементов (2.23) над $\mathbf{Q}$, получаем:

$$\mathbf{Norm}\left(\mathbf{Norm}_{\gamma}(a)\right) \mid \mathbf{Norm}_{\gamma}(\gamma - 1)^3 = 27,$$

что противоречит условию $f \neq 0 \pmod 3$.

Аналогично доказывается взаимная простота остальных элементов в условии леммы. ♦

Лемма 2.4 гарантирует возможность представления фактор-кольца $\mathbf{S}/\mathbf{f}$ в виде прямой суммы

$$\mathbf{S}/\mathbf{f} \equiv \mathbf{S}/\mathbf{p} \oplus \mathbf{S}/\mathbf{q} \oplus \mathbf{S}/\mathbf{r}$$

фактор-колец $\mathbf{S}/\mathbf{p}$, $\mathbf{S}/\mathbf{q}$, $\mathbf{S}/\mathbf{r}$ где $\mathbf{f} = (f)$, $\mathbf{p} = (P) = (f_1)$, $\mathbf{q} = (Q) = (f_2)$, $\mathbf{r} = (R) = (f_3)$ - главные идеалы, порожденные элементами f, $P = f_1$, $Q = f_2$, $R = f_3$, а также возможность вложения подкольца $\mathbf{Z}/f\mathbf{Z} \subset \mathbf{S}/\mathbf{f}$ в эту прямую сумму. Поэтому следующая лемма является частным случаем китайской теоремы об остатках. Её доказательство приводится только для явного описания такого вложения.

Лемма 2.5. *Для любого* $W \in \mathbf{Z}/f\mathbf{Z}$ *существуют эффективно определяемые элементы* $X, Y, Z \in \mathbf{S}/(f)$ *и константы* $a, b, c \in \mathbf{Z}/f\mathbf{Z}$ *такие, что:*

(a) справедливо сравнение

$$W \equiv aXQR + bYPR + cZPQ, \pmod{f}, \tag{2.24}$$

причем

$$X \equiv W \pmod{(P)},\ Y \equiv W \pmod{(Q)},\ Z \equiv W \pmod{(R)};$$

(b) числа X, Y, Z допускают представления в форме:

$$\begin{aligned} &X = X_1 + X_2\ \sqrt[3]{2} + X_3\ \overline{\gamma}\sqrt[3]{4};\\ &Y = Y_1 + Y_2\ \gamma\sqrt[3]{2} + Y_3\ \sqrt[3]{4};\\ &Z = Z_1 + Z_2\ \overline{\gamma}\sqrt[3]{2} + Z_3\ \gamma\sqrt[3]{4};\\ &0 \le X_1, Y_1, Z_1 < 2^{t+1};\quad 0 \le X_2, Y_2, Z_2, X_3, Y_3, Z_3 < 2^t\ . \end{aligned} \tag{2.25}$$

Доказательство. Соотношение (2.24) является следствием китайской теоремы об остатках. Для доказательства свойства (а) необходимо доказать, что $a,b,c \in \mathbf{Z}/f\mathbf{Z}$. Непосредственно проверяются равенства:

$$RQ = (P-3)P+3,\quad PR = (Q-3)Q+3,\quad PQ = (R-3)+3\ .$$

Поэтому для выполнения равенств

$$aQR \equiv 1 \pmod{P},\ bPR \equiv 1 \pmod{Q},\ cPQ \equiv 1 \pmod{R}$$

достаточно положить

$$a \equiv 3^{-1} \pmod{f},\quad b \equiv 3^{-1} \pmod{f},\quad c \equiv 3^{-1} \pmod{f}\ .$$

Опуская рутинные выкладки, связанные с применением метода неопределенных коэффициентов, приведем выражения для X_j, Y_j, Z_j $(j = 1, 2, 3)$ в форме:

$$\begin{cases} X_1 + (-X_3)\ 2^{t+1} + X_2\ 2^{2t+1} = (3a)^{-1}\ W\\ Y_1 + (-Y_3)\ 2^{t+1} + Y_2\ 2^{2t+1} = (3b)^{-1}\ W\\ Z_1 + (-Z_3)\ 2^{t+1} + Z_2\ 2^{2t+1} = (3c)^{-1}\ W \end{cases} \tag{2.26}$$

Из соотношений (2.26) эффективно определяются значения X_j, Y_j, Z_j . Действительно, пусть χ есть наименьший неотрицательный вычет для $(3a)^{-1}\ W \pmod{f}$. Пусть, как и ранее,

$\mathbf{quot}(u//v)$ и $\mathbf{exc}(u//v)$ – неполное частное и остаток от деления числа u на v соответственно. Тогда, например, для X_j имеем:

$$X_1 = \mathbf{exc}\left(\chi // 2^{t+1}\right),$$

$$X_2 = \mathbf{quot}\left(\chi - X_1 // 2^{2t+1}\right),$$

$$(-X_3) = (-X_1)\, 2^{-t-1} - X_2\, 2^t.$$

Нетрудно заметить, что элементы X_2, X_3 допускают t-битовое представление, а элемент X_1 допускает (t+1)-битовое представление. ♦

Рассмотрим первое из равенств (2.26). Пусть

$$X_1 = X_t^1 2^t + \ \ldots + X_0^1 2^0,$$

$$X_2 = X_{t-1}^2 2^{t-1} + \ \ldots + X_0^2 2^0,$$

$$X_3 = X_{t-1}^3 2^{t-1} + \ \ldots + X_0^3 2^0$$

есть битовые представления элементов X_1, X_2, X_3. Тогда соотношение (2.26) для X можно переписать в виде:

$$X = X_t^1 \left(\sqrt[3]{2}\right)^{3t} + X_{t-1}^2 \left(\sqrt[3]{2}\right)^{3t-1} + X_{t-1}^3 \left(\sqrt[3]{2}\right)^{3t-2} + \\ + X_{t-1}^1 \left(\sqrt[3]{2}\right)^{3t-3} + \ldots + X_0^1 \left(\sqrt[3]{2}\right)^0. \qquad (2.27)$$

Равенство (2.27) можно интерпретировать как представление элемента X "в системе счисления с основанием $\left(\sqrt[3]{2}\right)$", равенства, аналогичные (2.27), для Y и Z - как представления элементов Y и Z "в системах счисления с основанием $\gamma\left(\sqrt[3]{2}\right)$ и $\bar{\gamma}\left(\sqrt[3]{2}\right)$" соответственно.

Замечание 2.2. Несмотря на не вполне привычную терминологию ("системы счисления с комплексным иррациональным основанием"), никаких "приближенных" вычислений, конечно, не произ-

водится. Элементы, обозначенные $\left(\sqrt[3]{2}\right)$, $\gamma\left(\sqrt[3]{2}\right)$ и $\bar{\gamma}\left(\sqrt[3]{2}\right)$, есть просто три различных корня уравнения $W=1$ в фактор-кольце $\mathbf{S}/\mathbf{f}$. Такая (неформальная) интерпретация равенства (2.27) позволяет ввести простые правила преобразований ассоциированных кодов

$$< X >= (X_t^1, X_{t-1}^2, X_{t-1}^3, X_{t-1}^1, \ldots, X_0^1). \qquad (2.28)$$

Арифметические действия над элементами кольца $\mathbf{S}/\mathbf{f}$ индуцируют правила преобразования кодов (2.28): при сложении элементов коды преобразуются по правилу "перенос в старший разряд через две позиции"; умножение элемента X на $\left(\sqrt[3]{2}\right)$ равносильно циклическому сдвигу кода с инвертированием знака младшего бита и т.д., как и в случае обычной арифметики кольца вычетов $\left(\mathrm{mod}\, f_s\right)$.

Лемма 2.6. *Если число* $f = 2^B + 1$ *является нормальным числом Ферма, то функции*

$$h_m^1(n) = \left(\sqrt[3]{2}\right)^{mn},\ h_m^2(n) = \left(\gamma\sqrt[3]{2}\right)^{mn} \text{ и } h_m^3(n) = \left(\bar{\gamma}\sqrt[3]{2}\right)^{mn}$$

образуют ортогональные семейства:

$$\sum_{n=0}^{2B-1} h_m^{\nu}(n)\ h_k^{\nu}(q-n) = 2B\ \delta_{mk}(\mathrm{mod}\, \mathbf{J}_{\nu}), \qquad (2.29)$$

где $(\nu = 1,2,3)$, $\mathbf{J}_{\nu} = \mathbf{p},\mathbf{q},\mathbf{r}$ *соответственно.*

Доказательство. Единственной причиной нарушения равенства (2.29) может служить, например, для кольца $\mathbf{S}/\mathbf{p}$ необратимость элементов $\left(\sqrt[3]{2}\right)^{m-k} - 1 = \left(\sqrt[3]{2}\right)^{\tau} - 1$ при суммировании членов геометрической прогрессии. Этого не происходит, если $\mathbf{Norm}_{\gamma}\left(\left(\sqrt[3]{2}\right)^{\tau} - 1\right)$ есть число, взаимно простое с числом f_s.

Но при $\tau \neq 0 \pmod 3$ имеем:

$$\mathbf{Norm}_{\gamma}\left(\left(\sqrt[3]{2}\right)^{\tau}-1\right)=\left(\left(\sqrt[3]{2}\right)^{\tau}-1\right)\left(\gamma\left(\sqrt[3]{2}\right)^{\tau}-1\right)\left(\overline{\gamma}\left(\sqrt[3]{2}\right)^{\tau}-1\right)=2^{\tau}-1.$$

При $\tau \equiv 0 \pmod 3$ имеем

$$\mathbf{Norm}_{\gamma}\left(\left(\sqrt[3]{2}\right)^{\tau}-1\right)=\left(2^{\tau/3}-1\right)^{3},$$

и существование нетривиального общего делителя чисел $\mathbf{Norm}_{\gamma}\left(\left(\gamma^{u}\sqrt[3]{2}\right)^{\tau}-1\right)$ невозможно при u =0, 1, 2 и $\tau > 3$.

При $\tau = 1,2,3$ элементы $\left(\left(\gamma^{u}\sqrt[3]{2}\right)^{\tau}-1\right)$ являются единицами кольца **S** и, следовательно, обратимы в соответствующих факторкольцах. ♦

Определим оператор F левого сдвига Ферма ("перенос X_k в нулевой разряд с инвертированием знака") на множестве редуцированных кодов посредством равенства:

$$\mathrm{F}\ \langle X\rangle_{\mathbf{J}_{\nu}}=\langle X_{T-1},\ \ldots,\ X_0,\ -X_T\rangle.$$

Аналогично определялся обратный оператор (правого) сдвига Ферма:

$$\mathrm{F}^{-1}\langle X\rangle_{\mathbf{J}_{\nu}}=\langle -X_q,\ X_K,\ X_{K-1},\ \ldots,\ X_1\rangle.$$

Определение 2.4. Пусть $x(n)$ есть $2B$-периодическая последовательность элементов колец $\mathbf{S}/\mathbf{p}, \mathbf{S}/\mathbf{q}, \mathbf{S}/\mathbf{r}$; ν=1,2,3; $\mathbf{J}_{\nu}=\mathbf{p},\mathbf{q},\mathbf{r}$, Определим шифт-преобразование Ферма последовательности $x(n)$ равенствами:

$$\left\langle X_k(m)\right\rangle_{\mathbf{J}_{\nu}}=\sum_{n=0}^{2B-1}\mathrm{F}^{\,mn}\left\langle x(n)\right\rangle_{\mathbf{J}_{\nu}}\quad (m=0,\ 1,\ \ldots,\ T-1). \tag{2.30}$$

Аргументацией, аналогичной получению соотношения (2.19), нетрудно показать, что имеет место равенство

$$\left\langle (2B)\cdot x(n)\right\rangle_{\mathbf{J}_\nu} = \sum_{m=0}^{2B-1} \mathrm{F}^{-mn}\ \left\langle X_k(m)\right\rangle_{\mathbf{J}\nu}. \qquad (2.31)$$

Последнее равенство позволяет рассматривать преобразование (2.30), с точностью до нормирующего множителя $(2B)$, как обратное по отношению к (2.31) и наоборот.

2.3.2. Вычисление свертки по модулю составного числа Ферма

Для элементов, представленных в форме (2.25), положим (j=1,2,3) $X_j = \mathbf{Pr}_j^0 X, Y_j = \mathbf{Pr}_j^1 Y, Z_j = \mathbf{Pr}_j^2 Z.$ Тогда для произведения элементов A и B, заданных, например, в форме

$$A = \mathbf{Pr}_1^0 A + \sqrt[3]{2}\ \mathbf{Pr}_2^0 A + \sqrt[3]{4}\ \mathbf{Pr}_3^0 A,$$
$$B = \mathbf{Pr}_1^0 B + \sqrt[3]{2}\ \mathbf{Pr}_2^0 B + \sqrt[3]{4}\ \mathbf{Pr}_3^0 B,$$

справедливы соотношения типа свертки:

$$\begin{aligned}
\mathbf{Pr}_1^0 AB &= \mathbf{Pr}_1^0 A\cdot\mathbf{Pr}_1^0 B + 2\mathbf{Pr}_2^0 A\cdot\mathbf{Pr}_3^0 B + 2\mathbf{Pr}_3^0 A\cdot\mathbf{Pr}_2^0 B,\\
\mathbf{Pr}_2^0 AB &= \mathbf{Pr}_1^0 A\cdot\mathbf{Pr}_2^0 B + \mathbf{Pr}_2^0 A\cdot\mathbf{Pr}_1^0 B + 2\mathbf{Pr}_3^0 A\cdot\mathbf{Pr}_2^0 B, \qquad (2.32)\\
\mathbf{Pr}_3^0 AB &= \mathbf{Pr}_1^0 A\cdot\mathbf{Pr}_3^0 B + \mathbf{Pr}_3^0 A\cdot\mathbf{Pr}_1^0 B + \mathbf{Pr}_2^0 A\cdot\mathbf{Pr}_2^0 B.
\end{aligned}$$

Равенства (2.32) в сочетании с соотношением $\left(\sqrt[3]{2}\right)^B = \left(\sqrt[3]{2}\right)^{3t+1} \equiv -1\,(\mathrm{mod}\,\mathbf{p})$ и с аналогичными соотношениями для $\mathbf{Pr}_j^0, \mathbf{Pr}_j^0$ позволяют организовать "блочное" вычисление элементов фактор-колец $\mathbf{S}/\mathbf{p}, \mathbf{S}/\mathbf{q}, \mathbf{S}/\mathbf{r}$ с помощью несложной модификации арифметики Ферма, отличающейся от обычной несколько более усложненным правилом обмена старших битов между блоками.

Рассмотренные выше шифт-преобразования позволяют вычислять циклическую свертку целочисленных $2B$-периодических по-

следовательностей с помощью обычной спектральной схемы без умножений. Опуская детали описания такой схемы, сформулируем окончательный результат.

Теорема 2.2. Пусть нормальное число Ферма имеет вид: $f = 2^B + 1,\ B = 2^s = 3t + 1$. *Тогда для вычисления циклической свертки длины N = 2(3t + 1) достаточно выполнения:*

1) девяти (шести левых (прямых) и трех правых (обратных)) шифт-преобразований;

2) вычисления произведений компонент спектров шифт-преобразований;

3) реконструкции значений свертки по китайской теореме об остатках в форме (2.24). ♦

Замечание 2.3. Рассмотренный метод и синтезированные алгоритмы без существенной модификации переносятся и на случай нормальных чисел Ферма вида

$$f = 2^B + 1,\ B = 2^r = 3t - 1.$$

В этом случае используется альтернативное разложение числа Ферма в кольце

$$\mathbf{S}/\mathbf{f} \equiv \mathbf{S}/\mathbf{p} \oplus \mathbf{S}/\mathbf{q} \oplus \mathbf{S}/\mathbf{r},$$

где

$$\mathbf{p} = \left(2^t \ \sqrt[3]{1/2} + 1\right),\ \mathbf{q} = \left(2^t\gamma \ \sqrt[3]{1/2} + 1\right),\ \mathbf{r} = \left(2^t\bar{\gamma} \ \sqrt[3]{1/2} + 1\right),$$

а "дробь" $1/2$ понимается как элемент $2^{-1} \pmod f$.

В таблице 2.2 приведены разложения чисел $f = 2^k + 1,\ (1 \le k \le 32)$ на простые сомножители. Эти численные данные, данные таблиц монографии [34], показывают, что числа Ферма f_5, f_6, f_7 являются нормальными числами Ферма, что позволяет вычислять свертки длин 64, 128, 256 с помощью описанного метода.

Таблица 2.2

Факторизация чисел $f = 2^k + 1,\ (1 \le k \le 32)$

k	Факторизация	k	Факторизация
1	3	17	257^2
2	5	18	$5 \times 13 \times 37 \times 109$
3	3^2	19	3×174763
4	17	20	17×61681
5	3×11	21	$3^2 43 \times 5419$
6	5×13	22	$5 \times 397 \times 2113$
7	3×43	23	3×2796203
8	257	24	$97 \times 257 \times 673$
9	$3^3 19$	25	$3 \times 11 \times 251 \times 4051$
10	$5^2 41$	26	$5 \times 53 \times 157 \times 1613$
11	3×683	27	$3^2 19 \times 87211$
12	17×241	28	17×15790321
13	3×2731	29	$3 \times 59 \times 3033169$
14	$5 \times 29 \times 113$	30	$5^2 13 \times 41 \times 61 \times 1321$
15	$3^2 11 \times 331$	31	3×715827883
16	65537	32	641×6700417

ЧАСТЬ 3. КАНОНИЧЕСКИЕ СИСТЕМЫ СЧИСЛЕНИЯ В ПОЛЯХ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ И ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЯ СВЕРТКИ

> – Номер моего такси 1729. Мне кажется, что это довольно скучное число.
>
> – Нет-нет, Харди. Что вы? – тут же отвечал Рамануджан. – Это очень интересное число. Это наименьшее число, представимое суммой кубов двух чисел двумя различными способами.
>
> Ч.П.Сноу [1].

3.1. Введение, основные идеи

3.1.1. Требования, предъявляемые к системам счисления

В настоящей части мы рассмотрим возможность применения результатов, относительно недавно полученных венгерскими математиками [30]-[31] к решению задачи, рассматривавшейся уже в предыдущей части пособия, но, скорее, на эвристическом уровне.

Давайте перечислим те основные требования к частично уже рассмотренным в предыдущих разделах системам счисления, которые, с одной стороны, были бы "естественными" для машинного представления данных, а, с другой стороны, позволяли бы расширить круг эффективных алгоритмов решения задач, подобных рассмотренным в предыдущих главах.

---

[1] Из Предисловия Ч.П.Сноу к книге Г.Г.Харди "Апология математики", Изд-во РХД, *2000*

1. Возможность представления целых чисел n, по крайней мере, в виде конечной суммы

$$n = \sum_{j=-k(n)}^{K(n)} a_j \psi(j), \qquad (3.1)$$

где $k(n), K(n) \geq 0$ *- целые числа,* $\psi(j)$ *- вещественно- или комплекснозначная последовательность ("основание системы счисления"),* $a_j \in \mathrm{A} \subset \mathbf{C}$ *- "цифры", принадлежащие некоторому подмножеству комплексного поля ("алфавит").*

2. Возможность обобщения представления (3.1) *на подкольца комплексного поля* $\mathbf{C}$*, более общие, чем кольцо целых чисел.*

3. Множество $\mathrm{A} \subset \mathbf{C}$ *должно быть конечным и содержать "небольшое" число элементов.*

4. Возникающие при сложении чисел, представленных в форме (3.1) *"суммы цифр", не принадлежащие, возможно, алфавиту* A*, должны выражаться линейной комбинацией элементов основания системы счисления с коэффициентами из множества* A*.*

5. Возникающе при умножении чисел, представленных в форме (3.1)*, произведения* $\psi(j)\psi(i)$*, не являющиеся, возможно, элементами основания системы счисления, должны выражаться линейной комбинацией элементов основания системы счисления с коэффициентами из множества* A*.*

6. Представление (3.1) *должно быть "беззнаковым".*

7. Представление чисел в форме (3.1*) должно быть однозначным.*

Продолжая неформальное обсуждение, охарактеризуем значимость каждого из приведенных выше требований (пожеланий) к "хорошим" системам счисления. Важность этих требований для приложений весьма различна.

Действительно, первое условие представляется совершенно необходимым – у "компьютерной математики" и так достаточно проблем с конечноразрядным представлением *действительных* чисел. Второе условие диктуется надеждой на возможность вычислений в подкольцах комплексного поля (в конечномерных алгебрах, в частности) по аналогии с целочисленными вычислениями. Третье условие связано с аппаратной реализацией вычислительных алгоритмов. Четвертое и пятое условия, в отличие от первых трех, связаны не с "удобным" *представлением* чисел, а с желанием обеспечить эффективную реализацию арифметических операций. Шестое условие возникает из желания распространить понятие системы счисления на структуры, в которых не определено "естественное" упорядочение. Седьмое условие, как и шестое, желательно, но как уже продемонстрировано в предыдущих главах, не является абсолютно необходимым.

Основная идея. ***Раз уж простые числа с "хорошей" реализацией модулярных операций в двоичной системе счисления встречаются в натуральном ряду редко, а в части 2 пособия показана возможность синтеза эффективных параллельных алгоритмов, использующих альтернативное разложение составных модулей в полях алгебраических чисел, то давайте сами синтезируем модули специального вида, факторизующиеся по образцу факторизации, но ассоциированные с иными системами счисления в полях алгебраических чисел.***

3.2. Предварительные сведения

3.2.1. Целые элементы в квадратичных полях

Пусть $\mathbf{Q}\left(\sqrt{d}\right)$ есть *квадратичное поле*:

$$\mathbf{Q}\left(\sqrt{d}\right)=\left\{z=a+b\sqrt{d}\,;a,b\in\mathbf{Q}\right\}, \qquad (3.2)$$

где d - натуральное число, свободное от квадратов. Напомним, что при $d>0$ расширение (или квадратичное поле) называется *вещественным,* при $d<0$ - *мнимым.*

Напомним также, что если для элемента $z=a+b\sqrt{d}\in\mathbf{Q}\left(\sqrt{d}\right)$ *норма и след* есть целые числа:

$$\begin{aligned}&\mathbf{Norm}\left(z\right)=\left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right)=a^2-db^2\in\mathbf{Z},\\&\mathbf{Tr}\left(z\right)=\left(a+b\sqrt{d}\right)+\left(a-b\sqrt{d}\right)=2a\in\mathbf{Z},\end{aligned}\qquad(3.3)$$

то элемент называется *целым алгебраическим числом поля* $\mathbf{Q}\left(\sqrt{d}\right)$, в отличие от "обычных" целых чисел, которые называются *целыми рациональными числами*.

Классификация целых элементов поля $\mathbf{Q}\left(\sqrt{d}\right)$ описывается следующим утверждением (см., например, [32], [24]).

Лемма 3.1. *Целыми алгебраическими числами вещественного поля* $\mathbf{Q}\left(\sqrt{d}\right)$ *являются числа*

$$z=\begin{cases}a+b\sqrt{d}\,; & a,b\in\mathbf{Z},\text{ при }d\equiv 2,3\left(\bmod 4\right);\\ a+\dfrac{1}{2}b\left(\sqrt{d}-1\right); & a,b\in\mathbf{Z},\text{ при }d\equiv 1\left(\bmod 4\right).\end{cases}$$

♦

Пусть теперь $d<0,\quad \Delta=\left|d\right|$.

Лемма 3.2. *Целыми алгебраическими числами мнимого поля* $\mathbf{Q}\left(i\sqrt{\Delta}\right)$ *являются числа*

$$z=\begin{cases}a+bi\sqrt{\Delta}\,; & a,b\in\mathbf{Z},\text{ при }\Delta\equiv -2,-3\left(\bmod 4\right);\\ a+\dfrac{1}{2}b\left(i\sqrt{\Delta}-1\right); & a,b\in\mathbf{Z},\text{ при }\Delta\equiv -1\left(\bmod 4\right).\end{cases}$$

♦

3.2.2. "Канонические" системы счисления в квадратичных полях

В работах [30]-[31] введено понятие канонических систем счисления в кольце целых элементов квадратичных полей $\mathbf{Q}\left(\sqrt{d}\right)$.

Определение 3.1. Целое алгебраическое число $\alpha = A + \sqrt{d}$ называется *основанием канонической системы счисления* в кольце целых элементов поля $\mathbf{Q}\left(\sqrt{d}\right)$, если любой целый элемент этого поля однозначно представим в форме конечной суммы

$$z = \sum_{j=0}^{k(z)} z_j \alpha^j , \qquad (3.4)$$

$$z_j \in \mathrm{N} = \left\{0, 1, \ldots, \left|\mathbf{Norm}(\alpha)\right| - 1\right\}.$$

Пара $\left\{\alpha, \mathrm{N}\right\}$ называется *канонической системой счисления* в кольце целых поля $\mathbf{Q}\left(\sqrt{d}\right)$.

Далее кольцо целых элементов поля $\mathbf{Q}\left(\sqrt{d}\right)$ будем обозначать $\mathbf{S}\left(\sqrt{d}\right)$ или, если это не вызовет недоразумений, просто $\mathbf{S}$. Введем также обозначение:

$$\mathbf{Z}\left(\sqrt{d}\right) = \left\{z = a + b\sqrt{d} : a, b \in \mathbf{Z}\right\} \subseteq \mathbf{S}\left(\sqrt{d}\right) \subset \mathbf{Q}\left(\sqrt{d}\right).$$

В зависимости от того, является ли поле $\mathbf{Q}\left(\sqrt{d}\right)$ вещественным или мнимым, исчерпывающее описание канонических систем счисления дается следующими утверждениями, доказанными в [30]-[31].

Лемма 3.3. *Пусть поле* $\mathbf{Q}\left(\sqrt{d}\right)$ *- вещественное,* $0 < d \equiv 2, 3 \pmod 4$. *Тогда алгебраическое число* $\alpha = A \pm \sqrt{d}$

является основанием канонической системы счисления в кольце $\mathbf{S}\left(\sqrt{d}\right)=\mathbf{Z}\left(\sqrt{d}\right)$ *тогда и только тогда, когда*

$$0<-2A\le A^2-d\ge 2, \tag{3.5}$$

где A есть целое рациональное число. ♦

Лемма 3.4. *Пусть поле* $\mathbf{Q}\left(\sqrt{d}\right)$ *- вещественное,* $0<d\equiv 1\,(\mathrm{mod}\,4)$. *Тогда алгебраическое число* $\alpha=\frac{1}{2}\left(B\pm\sqrt{d}\right)$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right)\supset\mathbf{Z}\left(\sqrt{d}\right)$ *тогда и только тогда, когда B есть нечетное целое рациональное число и*

$$0<-B\le\frac{1}{4}\left(B^2-d\right)\ge 2 \tag{3.6}$$

♦

Лемма 3.5. *Пусть поле* $\mathbf{Q}\left(i\sqrt{\Delta}\right)$ *- мнимое,* $\Delta\equiv -2,-3\,(\mathrm{mod}\,4)$. *Тогда алгебраическое число* $\alpha=A+i\sqrt{\Delta}$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(i\sqrt{\Delta}\right)=\mathbf{Z}\left(i\sqrt{\Delta}\right)$ *тогда и только тогда, когда*

$$0\le -2A\le A^2+\Delta\ge 2, \tag{3.7}$$

где A есть целое рациональное число. ♦

Лемма 3.6. *Пусть поле* $\mathbf{Q}\left(i\sqrt{\Delta}\right)$ *- мнимое,* $\Delta\equiv -1\,(\mathrm{mod}\,4)$. *Тогда алгебраическое число* $\alpha=\frac{1}{2}\left(B\pm i\sqrt{\Delta}\right)$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right)\supset\mathbf{Z}\left(\sqrt{d}\right)$ *тогда и только тогда, когда*

$$0 \le -B \le \frac{1}{4}\left(B^2 + \Delta\right) \ge 2\,, \tag{3.8}$$

где B есть нечетное целое рациональное число. ♦

Замечание 3.1. Отметим, что представление целых алгебраических чисел в канонических системах счисления, в отличие от, например, двоичной системы счисления в кольце целых рациональных чисел не требует указания знака (±) числа. И положительные и отрицательные числа вещественного квадратичного поля записываются в "беззнаковой" форме (3.4). Это требование автоматически исключает из множества канонических систем, например кольца $\mathbf{Z}\left(\sqrt{2}\right)$, систему счисления с основанием $\alpha = \sqrt{2}$.

Следующие два утверждения описывают рекуррентный процесс определения "цифр" целого алгебраического числа в представлении (3.4) для канонических систем счисления.

Теорема 3.1. *Пусть* $d \ge 2$.

(а) при $d \equiv 2,3 \pmod 4$ *пусть* $\alpha = A \pm \sqrt{d}$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right) = \mathbf{Z}\left(\sqrt{d}\right)$; *пусть далее для*

$$z = z_1 + z_2\sqrt{d} \in \mathbf{S}\left(\sqrt{d}\right), \quad z_1, z_2 \in \mathbf{Z}$$

целые рациональные $s_k\left(z\right)$ *определены рекуррентными соотношениями:*

$$\begin{aligned} &s_{k+1}\left(z\right) = 2A\left[\frac{s_k\left(z\right)}{\mathbf{Norm}\left(\alpha\right)}\right] - \left[\frac{s_{k-1}\left(z\right)}{\mathbf{Norm}\left(\alpha\right)}\right], k \ge 0, \\ &s_{-1}\left(z\right) = \mp z_2\mathbf{Norm}\left(\alpha\right), \quad s_0\left(z\right) = z_1 \mp z_2 A. \end{aligned} \tag{3.9}$$

(b) при $d \equiv 1 \pmod 4$ *пусть* $\alpha = \frac{1}{2}\left(B \pm \sqrt{d}\ \right)$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right)$*; пусть далее для*

$$z = z_1 + \frac{1+\sqrt{d}}{2} z_2 \in \mathbf{S}\left(\sqrt{d}\right), \quad z_1, z_2 \in \mathbf{Z}$$

целые рациональные $s_k(z)$ *определены рекуррентными соотношениями:*

$$\begin{aligned} &s_{k+1}(z) = B\left[\frac{s_k(z)}{\mathbf{Norm}(\alpha)}\right] - \left[\frac{s_{k-1}(z)}{\mathbf{Norm}(\alpha)}\right], k \geq 0, \\ &s_{-1}(z) = \mp z_2 \mathbf{Norm}(\alpha), \quad s_0(z) = z_1 \mp z_2 \frac{B-1}{2}. \end{aligned} \tag{3.10}$$

Тогда

$$z = \sum_{j=0}^{k(z)} a_j(z) \alpha^j ,$$

где $a_j(z) \equiv s_j(z) \left(\mathrm{mod}\, \mathbf{Norm}(\alpha)\right)$. ♦

Теорема 3.2. *Пусть* $(-d) = \Delta \geq 2$.

(a) при $\Delta \equiv -2, -3 \pmod 4$ *пусть* $\alpha = A \pm \sqrt{d}$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(i\sqrt{\Delta}\right) = \mathbf{Z}\left(i\sqrt{\Delta}\right)$*; пусть далее для*

$$z = z_1 + z_2 i\sqrt{\Delta} \in \mathbf{S}\left(i\sqrt{\Delta}\right), \quad z_1, z_2 \in \mathbf{Z}$$

целые рациональные $s_k(z)$ *определены рекуррентными соотношениями:*

$$\begin{aligned} &s_{k+1}(z) = 2A\left[\frac{s_k(z)}{\mathbf{Norm}(\alpha)}\right] - \left[\frac{s_{k-1}(z)}{\mathbf{Norm}(\alpha)}\right], k \geq 0, \\ &s_{-1}(z) = \mp z_2 \mathbf{Norm}(\alpha), \quad s_0(z) = z_1 \mp z_2 A. \end{aligned} \tag{3.11}$$

(b) при $\Delta \equiv -1 \pmod 4$ *пусть* $\alpha = \frac{1}{2}\left(B \pm i\sqrt{\Delta}\ \right)$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(i\sqrt{\Delta}\right)$*; пусть далее для*

$$z = z_1 + \frac{1+i\sqrt{\Delta}}{2} z_2 \in \mathbf{S}\left(i\sqrt{\Delta}\right), \quad z_1, z_2 \in \mathbf{Z}$$

целые рациональные $s_k(z)$ *определены рекуррентными соотношениями:*

$$\begin{aligned} & s_{k+1}(z) = B\left[\frac{s_k(z)}{\mathbf{Norm}(\alpha)}\right] - \left[\frac{s_{k-1}(z)}{\mathbf{Norm}(\alpha)}\right], k \geq 0, \\ & s_{-1}(z) = \mp z_2 \mathbf{Norm}(\alpha), \quad s_0(z) = z_1 \mp z_2 \frac{B-1}{2}. \end{aligned} \tag{3.12}$$

Тогда

$$z = \sum_{j=0}^{k(z)} a_j(z)\alpha^j ,$$

где $a_j(z) \equiv s_j(z) \left(\mathrm{mod}\, \mathbf{Norm}(\alpha)\right)$. ♦

3.2.3. Примеры канонических систем счисления

Ясно, что плодотворность идеи представления данных в канонических системах счисления в контексте обсуждаемых проблем зависит от количества элементов множества N допустимых цифр и сложности преобразования целых чисел, не входящих в множество N, но возникающих при сложении и умножении элементов множества N. Таким образом, наиболее привлекательными являются такие канонические системы счисления в квадратичных полях, для которых $\mathbf{Norm}(\alpha) = 2,3$ и еще, может быть, $\mathbf{Norm}(\alpha) = 2^t$ с "разумно небольшим" $0 < t \in \mathbf{Z}$.. Таких квадратичных полей и канонических систем счисления в них относительно немного. Основываясь на Леммах 3.3 – 3.6, рассмотрим некоторые из них.

Пример 3.1. Пусть $\mathbf{Norm}(\alpha)=2$, тогда из неравенств (3.7) - (3.8) следует, что существует ровно три мнимых квадратичных поля, в кольцах целых элементов которых существуют бинарные канонические системы счисления, а именно:

(a) кольцо целых гауссовых чисел $\mathbf{Z}(i)\subset\mathbf{Q}(i)$ с основаниями, равными $\alpha=-1\pm i$;

(b) кольцо $\mathbf{S}(i\sqrt{7})\subset\mathbf{Q}(i\sqrt{7})$ с основаниями, равными $\alpha=\dfrac{-1\pm i\sqrt{7}}{2}$;

(c) кольцо $\mathbf{S}(i\sqrt{2})\subset\mathbf{Q}(i\sqrt{2})$ с основаниями, равными $\alpha=\pm i\sqrt{2}$;

Для вычислений в этих кольцах в канонических системах счисления необходимо получить представление целого рационального числа 2 в этих бинарных канонических системах. С использованием рекуррентных соотношений (3.11) Теоремы 3.4 получаем

(a) для кольца целых гауссовых чисел $\mathbf{Z}(i)$:

$$0\cdot\alpha^0+0\cdot\alpha^1+1\cdot\alpha^2+1\cdot\alpha^3=2\in\mathbf{Z}(i)$$

$$1\cdot\alpha^0+0\cdot\alpha^1+1\cdot\alpha^2+1\cdot\alpha^3+1\cdot\alpha^4=(-1)\in\mathbf{Z}(i);$$

(b) для кольца $\mathbf{S}(i\sqrt{7})$:

$$1\cdot\alpha^0+1\cdot\alpha^1+1\cdot\alpha^2+0\cdot\alpha^3+0\cdot\alpha^4+1\cdot\alpha^5+1\cdot\alpha^6+1\cdot\alpha^7=2\in\mathbf{S}(i\sqrt{7});$$

(c) для кольца $\mathbf{S}(i\sqrt{2})$:

$$0\cdot\alpha^0+0\cdot\alpha^1+1\cdot\alpha^2+0\cdot\alpha^3+1\cdot\alpha^4=2\in\mathbf{S}(i\sqrt{2}).$$

Пример 3.2. Пусть $\mathbf{Norm}(\alpha)=3$, тогда из неравенств (3.7) - (3.8) следует, что существуют только три мнимых квадратичных

поля, в кольцах целых элементов которых существуют тернарные канонические системы счисления, а именно:

(a) поле $\mathbf{Q}\left(i\sqrt{2}\right)$ с основаниями $\alpha = -1 \pm i\sqrt{2}$;

(b) поле $\mathbf{Q}\left(i\sqrt{3}\right)$ с основаниями $\alpha = \dfrac{-3 \pm i\sqrt{3}}{2}$;

(c) поле $\mathbf{Q}\left(i\sqrt{11}\right)$ с основаниями $\alpha = \dfrac{-1 \pm i\sqrt{11}}{2}$.

В этих случаях для вычислений в соответствующих кольцах в канонических системах счисления необходимо иметь представление целых рациональных чисел 3 и 4 в таких тернарных канонических системах, что также нетрудно получить с использованием рекуррентных соотношений (3.10) - (3.11) Теоремы 3.1.

Пример 3.3. Рассмотрим кольцо целых элементов $\mathbf{S}\left(\sqrt{d}\right) \subset \mathbf{Q}\left(\sqrt{d}\right), d > 0$ вещественного квадратичного поля.

При $d \equiv 1 \pmod 4$ пусть $\alpha = \dfrac{1}{2}\left(B \pm \sqrt{d}\ \right)$ является основанием канонической системы счисления в кольце $\mathbf{S}\left(\sqrt{d}\right)$. Тогда из соотношения (3.6) получаем

$$0 < -B \le \frac{1}{4}\left(B^2 - d\right) = \mathbf{Norm}\left(\alpha\right),$$

откуда легко следует, что минимально возможное значение нормы в правой части (3.6), для которого существуют основания $\alpha = \dfrac{1}{2}\left(B \pm \sqrt{d}\ \right)$ канонической системы счисления равно 4. В этом случае соответствующим полем и основаниями системы счисления являются $\mathbf{Q}\left(\sqrt{5}\right)$ и $\alpha = \dfrac{1}{2}\left(-5 \pm \sqrt{5}\ \right)$ соответственно.

Пусть $0 < d \equiv 2,3 \pmod 4$, $\alpha = A \pm \sqrt{d}$ является основанием канонической системы счисления в кольце $\mathbf{S}\left(\sqrt{d}\right) = \mathbf{Z}\left(\sqrt{d}\right)$. Тогда из соотношения (3.5) получаем

$$0 < -2A \le A^2 - d = \mathbf{Norm}\left(\alpha\right),$$

откуда легко следует, что минимально возможное значение нормы в правой части (3.13), для которого существуют основания канонической системы счисления $\alpha = A \pm \sqrt{d}$ равно 6. В этом случае соответствующим полем и основаниями системы счисления являются $\mathbf{Q}\left(\sqrt{3}\right)$ и $\alpha = -3 \pm \sqrt{3}$ соответственно.

3.3. Параллельные алгоритмы вычисления свертки в "канонических" системах счисления для квадратичных полей

3.3.1. Параллельные алгоритмы вычисления свертки в РКСС с основанием (i - 1)

Определение 3.7. Пусть $\alpha = -1 + i$. *Мерсенновским* $\mathbf{Z}(i)$-*числом* будем называть целое рациональное число M_n^1, представимое в форме

$$M_n^1 = \left(\alpha^n - 1\right)\left(\overline{\alpha^n} - 1\right) = 2^n - \left(\alpha^n + \overline{\alpha^n}\right) + 1; \qquad (3.13)$$

$\mathbf{Z}(i)$-*числом Ферма* будем называть целое рациональное число F_n^1, представимое в форме

$$F_n^1 = \left(\alpha^n + 1\right)\left(\overline{\alpha^n} + 1\right) = 2^n + \left(\alpha^n + \overline{\alpha^n}\right) + 1. \qquad (3.14)$$

Так как

$$\alpha = i - 1 = \sqrt{2}\left(\exp\left\{2\pi i / 8\right\}\right)^3, \qquad (3.15)$$

то явное выражение для чисел M_n^1 и F_n^1 определяется в зависимости от $n=8q+r, 0\le r\le 7$. Непосредственным вычислением находим:

$$M_{8q+0}^1 = 2^{8q} - 2\cdot 2^{4q} + 1, \qquad F_{8q+0}^1 = 2^{8q} + 2\cdot 2^{4q} + 1,$$
$$M_{8q+1}^1 = 2^{8q+1} + 2^{4q+1} + 1, \qquad F_{8q+1}^1 = 2^{8q+1} - 2^{4q+1} + 1,$$
$$M_{8q+2}^1 = 2^{8q+2} + 1, \qquad F_{8q+2}^1 = 2^{8q+2} + 1,$$
$$M_{8q+3}^1 = 2^{8q+3} - 2^{4q+2} + 1, \qquad F_{8q+3}^1 = 2^{8q+3} + 2^{4q+2} + 1,$$
$$M_{8q+4}^1 = 2^{8q+4} + 2\cdot 2^{4q+2} + 1, \qquad F_{8q+4}^1 = 2^{8q+4} - 2\cdot 2^{4q+2} + 1,$$
$$M_{8q+5}^1 = 2^{8q+5} - 2^{4q+3} + 1, \qquad F_{8q+5}^1 = 2^{8q+5} + 2^{4q+3} + 1,$$
$$M_{8q+6}^1 = 2^{8q+6} + 1, \qquad F_{8q+6}^1 = 2^{8q+6} + 1,$$
$$M_{8q+7}^1 = 2^{8q+7} + 2^{4q+4} + 1. \qquad F_{8q+7}^1 = 2^{8q+7} - 2^{4q+4} + 1.$$

Следует отметить, для чисел F_n^1, M_n^1 число (-1) является квадратичным вычетом $\left(\mathrm{mod}\, F_n^1\right), \left(\mathrm{mod}\, M_n^1\right)$ соответственно.

Таким образом, представление чисел F_n^1, M_n^1 в форме (3.13)-(3.14) приводит, как и в разделе 3.2, только к альтернативному представлению разложения (составного) чисел F_n^1, M_n^1 на множители.

Лемма 3.7. *При* $n\ne 0(\mathrm{mod}\, 4)$ *сомножители* $\left(\alpha^n \pm 1\right), \left(\overline{\alpha^n} \pm 1\right)$ *в* (3.51)-(3.14) *взаимно просты.*

Доказательство. Существование нетривиального общего делителя *A* у элементов $\left(\alpha^n \pm 1\right)$ и $\left(\overline{\alpha^n} \pm 1\right)$ влечет существование этого же делителя как у их произведений – чисел F_n^1, M_n^1, так и у их разностей

$$D_{\pm} = \left(\alpha^n \pm 1\right) - \left(\overline{\alpha^n} \pm 1\right) = \alpha^n - \overline{\alpha^n}.$$

Заметим, что

$$\left(\alpha^n \pm 1\right)\left(\overline{\alpha^n} \pm 1\right) \equiv 1 \left(\mathrm{mod}\, 2\right). \qquad (3.16)$$

С другой стороны, с учетом (3.15) имеем при $n \neq 0 \left(\mathrm{mod}\, 4\right)$

$$D_{\pm} = \alpha^n - \overline{\alpha^n} = 2i\left(\sqrt{2}\right)^n \mathrm{Im}\left(\xi\right),$$

где ξ - невещественный корень восьмой степени, следовательно

$$D_{\pm}^2 = \left(2\left(\sqrt{2}\right)^n i\, \mathrm{Im}\left(\xi\right)\right)^2 = -2^{n+2}\left(\mathrm{Im}\left(\xi\right)\right)^2$$

является степенью двойки, что противоречит (3.15). ♦

Далее, как и в разделе 3.2, введем понятие нормальных чисел F_n^1, M_n^1.

Определение 3.8. При $n \neq 0 \left(\mathrm{mod}\, 4\right)$ числа F_n^1, M_n^1 будем называть *нормальными*, если выполняются условия:

- при всех $1 < s < n$ числа $F_n^1 \left(\text{или}\, M_n^1\right)$ и F_s^1 (M_s^1 соответственно) взаимно просты;
- элемент $2n$ обратим в кольце $\mathbf{Z}/F_n^1\mathbf{Z}$ (или элемент n в кольце $\mathbf{Z}/M_n^1\mathbf{Z}$ соответственно).

В таблицах 3.1 – 3.2 приведены разложения чисел F_N^1, M_N^1 $\left(1 \le N \le 40\right)$ на множители. Индексы нормальных чисел выделены. Для свертки длины $2N$ по модулю нормального числа F_N^1 (или длины N по модулю нормального числа M_N^1) возможно ее параллельное вычисление методом, аналогичным описанному в разделе 3.2 с понятными коррективами в отношении реализации арифметических операций (см. Пример 3.1).

Таблица 3.1

Факторизация чисел $F_N^1\ (1 \le N \le 40)$

N	**Факторизация**	*N*	**Факторизация**
1	1	21	$13\times113\times1429$
2	5	22	$5\times397\times2113$
3	13	**23**	277×30269
4	3^2	24	17^2141^2
5	41	25	$41\times101\times8101$
5	5×13	26	$5\times53\times157\times1613$
7	113	27	$13\times37\times279073$
8	17^2	28	$3^243^2127^2$
9	3×37	**29**	536903681
10	5^241	30	$5^213\times41\times61\times1321$
11	2113	**31**	384773×5581
12	3^47^2	32	65537^2
13	53×157	33	$13\times312709\times2113$
14	$5\times29\times113$	34	$5\times137\times953\times26317$
15	$13\times41\times61$	35	$41\times113\times7416361$
16	257^2	36	$3^67^219^273^2$
17	137×953	**37**	593×231769777
18	$5\times13\times37\times109$	38	$5\times229\times457\times525313$
19	525313	39	$13^253\times157\times313\times1249$
20	$3^211^231^2$	40	17^261681^2

Для чисел M_N^1 ситуация несколько сложнее. Все числа M_N^1 $(1 \le N \le 40)$ имеют общий множитель, равный 5 (см. таблицу 3.2). Это может привести к нарушению ортогональности базисных функций

$$h_m^{\pm}(t) = (\pm i - 1)^{mt}$$

дискретных ТЧП, вычисляемых по $\left(\mathrm{mod}\left(\alpha^N-1\right)\right),\left(\mathrm{mod}\left(\overline{\alpha^N}-1\right)\right)$.

Тем не менее указанную трудность можно преодолеть. Действительно, пусть $M_N^1 \neq 0(\mathrm{mod}\,5)$, а неотрицательные целочисленные последовательности $x(n), y(n)$ и число M_N^1 удовлетворяют неравенству

$$\frac{1}{5}M_N^1 = M > N \max_{0\le n<N}\{x(n)\}\max_{0\le n<N}\{y(n)\}. \qquad (3.17)$$

Тогда значения компонент свертки

$$z(k) = (x * y)(k) = \sum_{n=0}^{N-1} x(n)y(k-n) \in \mathbf{Z} \qquad (3.18)$$

совпадают с их наименьшими неотрицательными вычетами $(\mathrm{mod}\,M)$.

Пусть $z_5(k)$ - результат вычисления $(\mathrm{mod}\,5)$ свертки (3.18), гипотетически полученный независимым методом. Результат $Z(k)$ - вычисления свертки с помощью шифт-преобразований с распараллеливанием в кольцах классов вычетов по $\left(\mathrm{mod}\left(\alpha^N-1\right)\right)$, $\left(\mathrm{mod}\left(\overline{\alpha^N}-1\right)\right)$ является "ошибочным" – числа M_N^1 не являются нормальными (нарушается второе условие). Но, по крайней мере, для нечетных значений N (в пределах таблицы 3.2) числа $\frac{1}{5}M_N^1 = M$ не делятся на 4.

Поэтому по китайской теореме об остатках для $a,b \in \mathbf{Z}$ с условиями $5a \equiv 1(\mathrm{mod}\,M)$, $Mb \equiv 1(\mathrm{mod}\,5)$ выполняется соотношение

$$Z(k) \equiv 5az(k) + Mbz_5(k)\left(\mathrm{mod}\,M_N^1\right),$$

откуда следует, что "автоматически", независимо от $z_5(k)$, справедливы сравнения

$$Z(k) \equiv 5az(k) + Mbz_5(k) \left(\mathrm{mod} M_N^1\right), Z(k) \equiv z(k) (\mathrm{mod} M).$$

То есть истинное значение $z(k)$ свертки получается редуцированием $Z(k)$ по $(\mathrm{mod} M)$.

Таблица 3.2

Факторизация чисел $M_N^1, (1 \le N \le 40)$

N	**Факторизация**	*N*	**Факторизация**
1	5	21	$5 \times 29 \times 14449$
2	5	22	$5 \times 397 \times 2113$
3	5	**23**	$5 \times 1013 \times 1657$
4	5^2	24	$3^4 5^2 7^2 13^2$
5	5^2	25	$5^3 268501$
6	5×13	**26**	$5 \times 53 \times 157 \times 1613$
7	5×29	27	$5 \times 109 \times 246241$
8	$3^2 5^2$	28	$5^2 29^2 113^2$
9	5×109	**29**	5×107367629
10	$5^2 \times 41$	30	$5^2 \times 13 \times 41 \times 61 \times 1329$
11	5×397	**31**	$5 \times 49477 \times 8681$
12	$5^2 \times 13^2$	32	$3^2 5^2 17^2 257^2$
13	5×1613	33	$5 \times 397 \times 4327489$
14	$5 \times 29 \times 113$	**34**	$5 \times 137 \times 953 \times 26317$
15	$5^2 \times 1321$	35	$5^2 29 \times 47392381$
16	$3^2 5^2 17^2$	36	$5^2 13^2 37^2 109^2$
17	5×26317	**37**	$5 \times 149 \times 184481113$
18	$5 \times 13 \times 37 \times 109$	38	$5 \times 229 \times 457 \times 525313$
19	$5 \times 229 \times 457$	39	$5 \times 1613 \times 21841 \times 3121$
20	$5^4 41^2$	40	$3^2 5^4 11^2 31^2 41^2$

3.3.2. Параллельные алгоритмы вычисления свертки в РКСС с основанием $\frac{1}{2}\left(-1\pm i\sqrt{7}\right)$

Определение 3.9. *Мерсенновским* $\mathbf{S}\left(i\sqrt{7}\right)$*-числом* будем называть целое рациональное число M_n^7, представимое в форме

$$M_n^7=\left(\alpha^n-1\right)\left(\overline{\alpha^n}-1\right)=2^n-\left(\alpha^n+\overline{\alpha^n}\right)+1;$$

$\mathbf{S}\left(i\sqrt{7}\right)$*-числом Ферма* будем называть целое рациональное число F_n^7, представимое в форме

$$F_n^7=\left(\alpha^n+1\right)\left(\overline{\alpha^n}+1\right)=2^n+\left(\alpha^n+\overline{\alpha^n}\right)+1,$$

где $\alpha=\frac{1}{2}\left(-1+i\sqrt{7}\right)$.

Введем далее понятие псевдонормальных чисел F_n^7, M_n^7, несколько отличающееся от понятия нормального числа, данного в Определении 3.8.

Определение 3.9. Числа F_n^7, M_n^7 будем называть *псевдонормальными*, если выполняются условия:

- при всех $1<s<n$ числа F_n^7 $\left(\text{или } M_n^7\right)$ и F_s^7 $\left(M_s^7, \text{соответственно}\right)$ имеют не более одного фиксированного общего делителя, равного d;
- числа F_n^7 $\left(\text{или } M_n^7\right)$ не делятся на квадрат целого рационального числа, отличного от d;
- элемент n обратим в кольце

$$\mathbf{z}\Big/d^{-1}F_n^7\mathbf{z}\left(\text{ или в кольце }\mathbf{z}\Big/d^{-1}M_n^7\mathbf{z}\right).$$

В таблицах 3.3 и 3.4 индексы псевдонормальных чисел $M_N^7, F_N^7\ (1 \le N \le 40)$ подчеркнуты.

Таблица 3.3

Факторизация чисел $F_N^7\ (1 \le N \le 40)$

N	**Факторизация**	*N*	**Факторизация**
1	2	21	$2 \times 7^3 43 \times 71$
2	2	**22**	2×2097349
3	2×7	**23**	2×4196903
4	2×3^2	24	$2 \times 113 \times 74209$
5	2×11	25	$2 \times 11 \times 1051 \times 1451$
6	2×37	26	$2 \times 53 \times 633257$
7	2×71	27	$2 \times 7 \times 37 \times 109 \times 2377$
8	2×113	28	$2 \times 3^2 2017 \times 7393$
9	$2 \times 7 \times 37$	**29**	$2 \times 6323 \times 42457$
10	2×541	30	$2 \times 37 \times 541 \times 26821$
11	2×991	**31**	$2 \times 41231 \times 26041$
12	$2 \times 3^4 5^2$	**32**	$2 \times 193 \times 11127041$
13	$2 \times 53 \times 79$	33	$2 \times 7 \times 67 \times 991 \times 9241$
14	$2 \times 29 \times 281$	**34**	$2 \times 137 \times 62699333$
15	$2 \times 7 \times 11 \times 211$	35	$2 \times 11 \times 71^2 491 \times 631$
16	2×32993	36	$2 \times 3^6 5^2 1885321$
17	2×65587	**37**	$2 \times 260999 \times 263293$
18	$2 \times 37 \times 3529$	**38**	$2 \times 64555541 \times 2129$
19	2×262543	39	$2 \times 7 \times 53 \times 79^2 118717$
20	$2 \times 3^2 58321$	40	$2 \times 113 \times 401 \times 12132401$

Возможность распараллеливания вычислений свертки и применения методики предыдущих разделов определяется тем, являются ли алгебраические числа

$$\left(\left(-1+i\sqrt{7}\right)^N \pm 1\right) \text{ и } \left(\left(-1-i\sqrt{7}\right)^N \pm 1\right)$$

взаимно простыми в кольце $\mathbf{S}\left(i\sqrt{7}\right)$.

Лемма 3.8. *Существуют числа* F_n^7, *для которых взаимно просты в* $\mathbf{S}\left(i\sqrt{7}\right)$ *элементы*

$$\beta_n = \left(\left(-1+i\sqrt{7}\right)^n + 1\right) \text{ и } \overline{\beta}_n = \left(\left(-1-i\sqrt{7}\right)^n + 1\right).$$

Доказательство. Допустим противное. Пусть

$\beta_n = \lambda\beta_n^+, \overline{\beta}_n = \lambda\beta_n^-$.

Но тогда либо $\lambda \in \mathbf{Z}$, либо справедливы соотношения

$\beta_n = \lambda\overline{\lambda}\gamma_n^+ = \mathbf{Norm}(\lambda)\gamma_n^+,\ \overline{\beta}_n = \lambda\overline{\lambda}\gamma_n^- = \mathbf{Norm}(\lambda)\gamma_n^-,\ \mathbf{Norm}(\lambda) \in \mathbf{Z}$,

то есть и в одном, и в другом случае общим делителем может быть только целое рациональное число $\mathbf{Norm}\left(\lambda\right)$. Но тогда $F_n^7 = \beta_n\overline{\beta}_n = \left(\mathbf{Norm}(\lambda)\right)^2\gamma_n^+\gamma_n^-$. То есть F_n^7 делится на квадрат целого рационального числа, что при $\mathbf{Norm}\left(\lambda\right) \neq \pm 1$ для чисел таблицы 3.3 имеет место только для значений $N = n = 4,12,20,28,35,36,39$, при которых F_n^7 не являются псевдонормальными. ♦

Как и числа M_N^1, псевдонормальные числа F_N^7 имеют общий множитель, равный 2. Кроме того, нормирующий множитель для шифт-преобразований равен *2N* и необратим в кольце $\mathbf{z}/F_n^7\mathbf{z}$. Проблема неортогональности базисных функций $h_m^{\pm}(t) = \frac{1}{2}\left(\pm i\sqrt{7}-1\right)^{mt}$

решается аналогично случаю чисел M_n^1. Пусть неотрицательные целочисленные последовательности $x(n), y(n)$ и число F_N^7 удовлетворяют неравенству

$$\frac{1}{2}F_N^7 = F > (2N)^2 \max_{0\le n<2N}\{x(n)\}\max_{0\le n<2N}\{y(n)\}. \qquad (3.19)$$

Тогда значения компонент свертки

$$2N\cdot z(k) = 2N\cdot(x*y)(k) = 2N\sum_{n=0}^{2N-1} x(n)y(k-n)\in \mathbf{Z} \qquad (3.20)$$

совпадают с их наименьшими неотрицательными вычетами $(\mathrm{mod}\,F)$. Пусть $2N\cdot z_2(k)$ - результат вычисления $(\mathrm{mod}\,2)$ свертки (3.20), гипотетически полученный независимым методом. Результат $2N\cdot Z(k)$ вычисления свертки с помощью шифт-преобразований с распараллеливанием в кольцах классов вычетов по $\left(\mathrm{mod}\left(\alpha^N-1\right)\right), \left(\mathrm{mod}\left(\overline{\alpha^N}-1\right)\right)$ является "ошибочным" Но, по крайней мере, для неисключительных значений N (в пределах таблицы 3.4) числа $\frac{1}{2}F_N^7 = F$ не делятся на 2. Поэтому по китайской теореме об остатках для $a,b\in\mathbf{Z}$ с условиями $2a\equiv 1(\mathrm{mod}\,F)$, $Fb\equiv 1(\mathrm{mod}\,2)$ выполняется соотношение

$$2N\cdot Z(k)\equiv 2az(k)\cdot 2N + Fbz_2(k)\cdot 2N\left(\mathrm{mod}\,F_N^7\right),$$

откуда следует, что справедливо сравнение

$$Z(k)\cdot 2N\equiv z(k)\cdot 2N(\mathrm{mod}\,F),$$

причем элемент $2N$ обратим в кольце $\mathbf{Z}/F\mathbf{Z}$. Отсюда следует, что $Z(k)\equiv z(k)(\mathrm{mod}\,F)$, то есть истинное значение $z(k)$ свертки получается редуцированием $Z(k)$ по $(\mathrm{mod}\,F)$.

Псевдонормальные числа M_N^7 из таблицы 3.4 делятся на 4, то есть на квадрат целгого числа. Но это целое число $d=4$ для псевдонормальных чисел является единственным квадратом, их делящим. Поэтому реконструкция истинного $z(k)$ возможна и в этом случае. Действительно, пусть неотрицательные целочисленные последовательности $x(n), y(n)$ и число M_N^7 удовлетворяют неравенству

$$\frac{1}{4}M_N^7 = M > N^2 \max_{0\le n<N}\{x(n)\}\max_{0\le n<N}\{y(n)\}.$$

Тогда значения компонент (ненормированной) свертки

$$N\cdot z(k) = N\cdot(x*y)(k) = N\cdot\sum_{n=0}^{N-1}x(n)y(k-n)\in\mathbf{Z} \qquad (3.21)$$

совпадают с их наименьшими неотрицательными вычетами $(\mathrm{mod}\,M)$. Пусть $z_4(k)$ - результат вычисления $(\mathrm{mod}\,4)$ свертки (3.21), полученный независимым методом. Результат $N\cdot Z(k)$ вычисления свертки с помощью шифт-преобразований с распараллеливанием в кольцах по $\left(\mathrm{mod}\left(\alpha^N-1\right)\right)$, $\left(\mathrm{mod}\left(\overline{\alpha^N}-1\right)\right)$ является "ошибочным". Но для неисключительных значений N в пределах таблицы 3.4 числа $\frac{1}{4}M_N^7 = M$ не делятся на 4. Поэтому по китайской теореме об остатках для $a,b\in\mathbf{Z}$ с условиями $4a\equiv 1(\mathrm{mod}M)$, $Mb\equiv 1(\mathrm{mod}\,4)$ выполняются соотношения

$$N\cdot Z(k)\equiv N\cdot 4az(k)+N\cdot Mbz_4(k)\left(\mathrm{mod}M_N^7\right),$$

$$N\cdot Z(k)\equiv N\cdot 4az(k)+N\cdot Mbz_4(k)\left(\mathrm{mod}M_N^7\right),\ Z(k)\equiv z(k)(\mathrm{mod}M).$$

То есть истинное значение $z(k)$ свертки получается редуцированием $Z(k)$ по $(\mathrm{mod}\,M)$.

Таблица 3.4

Факторизация чисел M_N^7 $(1 \le N \le 40)$

N	**Факторизация**	*N*	**Факторизация**
1	2^2	21	$2^2 29 \times 43 \times 421$
2	2^3	22	$2^3 23^2 991$
3	2^2	**23**	$2^2 2095853$
4	2^4	24	$2^5 3^4 5^2 7 \times 37$
5	$2^2 11$	25	$2^2 11 \times 151 \times 5051$
6	$2^3 7$	26	$2^3 53 \times 79 \times 2003$
7	$2^2 29$	27	$2^2 127 \times 163 \times 1621$
8	$2^5 3^2$	28	$2^4 29^2 71 \times 281$
9	$2^2 127$	**29**	$2^2 16067 \times 8353$
10	$2^3 11^2$	30	$2^3 7 \times 11^2 211 \times 751$
11	$2^2 23^2$	**31**	$2^2 373 \times 1439393$
12	$2^4 7 \times 37$	32	$2^7 3^2 113 \times 32993$
13	$2^2 2003$	33	$2^2 23^2 67 \times 60589$
14	$2^3 29 \times 71$	34	$2^3 137 \times 239 \times 65587$
15	$2^2 11 \times 751$	35	$2^2 11 \times 29 \times 1051 \times 25621$
16	$2^6 3^2 113$	36	$2^4 7 \times 37^2 127 \times 3529$
17	$2^2 137 \times 239$	37	$2^2 149 \times 230603167$
18	$2^3 7 \times 37 \times 127$	38	$2^3 262543 \times 130873$
19	$2^2 130873$	39	$2^2 68616367 \times 2003$
20	$2^4 11^2 541$	40	$2^5 3^2 11^2 541 \times 58321$

3.3.3. Параллельные алгоритмы вычисления свертки в РКСС с основанием $\left(\pm i\sqrt{2}\right)$

Определение 3.10. *Мерсенновским* $\mathbf{S}\left(i\sqrt{2}\right)$*-числом* будем называть целое рациональное число M_n^2, представимое в форме

$$M_n^2=\left(\alpha^n-1\right)\left(\overline{\alpha^n}-1\right)=2^n-\left(\alpha^n+\overline{\alpha^n}\right)+1;$$

$\mathbf{S}\left(i\sqrt{2}\right)$*-числом Ферма* будем называть целое рациональное число F_n^2, представимое в форме

$$F_n^2=\left(\alpha^n+1\right)\left(\overline{\alpha^n}+1\right)=2^n+\left(\alpha^n+\overline{\alpha^n}\right)+1,$$

где $\alpha=i\sqrt{2}$.

Заметим, что

$$F_n^2=\begin{cases}\left(2^{2t}-1\right)^2 & \text{при } n=4t;\\ 2^{4t+1}+1 & \text{при } n=4t+1;\\ \left(2^{2t+1}+1\right)^2 & \text{при } n=4t+2;\\ 2^{4t+3}+1 & \text{при } n=4t+3;\end{cases}\qquad M_n^2=\begin{cases}\left(2^{2t}+1\right)^2 & \text{при } n=4t;\\ 2^{4t+1}+1 & \text{при } n=4t+1;\\ \left(2^{2t+1}-1\right)^2 & \text{при } n=4t+2;\\ 2^{4t+3}+1 & \text{при } n=4t+3,\end{cases}$$

то есть при четных n числа F_n^2, M_n^2 являются точными квадратами, а при нечетных n справедливо равенство $F_n^2=M_n^2$, причем числа F_n^2, M_n^2 имеют вид $2^{\mu}+1$. Поэтому содержание данного раздела является нетривиальным в той степени, в какой возможно распространение методики раздела 3 на "фермаподобные" числа $F_n^2=M_n^2=2^{4t+\nu}+1$ при $\nu=1,3$. Факторизация чисел указанного вида приведена в таблице 3.2 (см. также [35]). Приведем ее еще раз только для нечетных $n=N$.

Далее, как и в предыдущем разделе, введем понятие псевдонормальных чисел F_n^2, M_n^2.

Определение 3.11. Числа F_n^2, M_n^2 будем называть *псевдонормальными*, если выполняются условия:

- при всех $1 < s < n$ числа F_n^2 (или M_n^2) и F_s^2 (или M_s^2 соответственно) имеют не более одного фиксированного общего делителя, равного d;
- числа F_n^2, M_n^2 не делятся на квадрат целгого рационального числа, отличного от d;
- элемент n обратим в кольце $\mathbf{Z}/d^{-1}F_n^2\mathbf{Z}$ (или в кольце $\mathbf{Z}/d^{-1}M_n^2\mathbf{Z}$).

Таблица 3.4

Факторизация чисел 2^N+1 $(1 \le N \le 32)$

N	**Факторизация**	*N*	**Факторизация**
1	3	17	257^2
3	3^2	**19**	3×174763
5	3×11	21	$3^2 43\times 5419$
7	3×43	**23**	3×2796203
9	$3^3 19$	25	$3\times 11\times 251\times 4051$
11	3×683	27	$3^2 19\times 87211$
13	3×2731	**29**	$3\times 59\times 3033169$
15	$3^2 11\times 331$	**31**	3×715827883

В таблице 3.5 индексы псевдонормальных чисел M_n^2, F_n^2 $(1 \le n \le 31)$ подчеркнуты.

Как и ранее, возможность распараллеливания вычислений свертки и применения методики предыдущих разделов определяется тем, являются ли алгебраические числа

$\left(\left(i\sqrt{2}\right)^N \pm 1\right)$ и $\left(\left(i\sqrt{2}\right)^N \pm 1\right)$

взаимно простыми в кольце $\mathbf{S}\left(i\sqrt{2}\right)$.

Лемма 3.9. *Существуют числа* F_n^2 *для которых взаимно просты в* $\mathbf{S}\left(i\sqrt{2}\right)$ *элементы*

$$\beta_n = \left(\left(i\sqrt{2}\right)^n + 1\right) \text{ и } \overline{\beta}_n = \left(\left(-i\sqrt{2}\right)^n + 1\right).$$

Доказательство. Аналогично доказательству Леммы 3.8, пусть $\beta_n = \lambda\beta_n^+, \overline{\beta}_n = \lambda\beta_n^-$. Тогда либо $\lambda \in \mathbf{Z}$, либо справедливы соотношения

$$\beta_n = \lambda\overline{\lambda}\gamma_n^+ = \mathbf{Norm}(\lambda)\gamma_n^+,\ \overline{\beta}_n = \lambda\overline{\lambda}\gamma_n^- = \mathbf{Norm}(\lambda)\gamma_n^-,\ \mathbf{Norm}(\lambda) \in \mathbf{Z}$$

,

то есть и в одном, и в другом случае общим делителем может быть только целое рациональное число $\mathbf{Norm}(\lambda)$. Но тогда $F_n^2 = \beta_n\overline{\beta}_n = \left(\mathbf{Norm}(\lambda)\right)^2\gamma_n^+\gamma_n^-$, то есть F_n^2 делится на квадрат целого рационального числа, что при $\mathbf{Norm}(\lambda) \neq \pm 1$ для n в пределах таблицы 3.5 не имеет места при $n = 1,5,7,11,13,19,23,29,31$. ♦

То есть псевдонормальные числа $F_n^2 = M_n^2$ имеют общий множитель, равный 3. Кроме того, нормирующий множитель для шифт-преобразований равен *2N* для чисел F_N^2 и равен *N* для чисел M_N^2. Числа *2N* и *N* обратимы в кольцах $\mathbf{z}/F_N^2\mathbf{z} = \mathbf{z}/M_N^2\mathbf{z}$. Проблема неортогональности базисных функций $h_m^{\pm}(t) = \left(\pm i\sqrt{2}\right)^{mt}$ решается аналогично случаю чисел M_N^1. Пусть неотрицательные целочис-

ленные последовательности $x(n), y(n)$ и, например, число F_N^2 удовлетворяют неравенству

$$\frac{1}{3}F_N^2 = F > (2N)^2 \max_{0\le n<2N}\{x(n)\}\max_{0\le n<2N}\{y(n)\}. \qquad (3.22)$$

Тогда значения компонент свертки

$$2N\cdot z(k) = 2N\cdot(x*y)(k) = 2N\sum_{n=0}^{2N-1} x(n)y(k-n)\in \mathbf{Z}, \qquad (3.23)$$

совпадают с их наименьшими неотрицательными вычетами $(\mathrm{mod}\,F)$. Пусть $2N\cdot z_2(k)$ - результат вычисления $(\mathrm{mod}\,3)$ свертки (3.23), гипотетически полученный независимым методом. Результат $2N\cdot Z(k)$ вычисления свертки с помощью шифт-преобразований с распараллеливанием в кольцах классов вычетов по $\left(\mathrm{mod}\left(\alpha^N-1\right)\right), \left(\mathrm{mod}\left(\overline{\alpha^N}-1\right)\right)$ является "ошибочным" Но, по крайней мере, для неисключительных значений N (в пределах таблицы 3.5) числа $\frac{1}{3}F_N^2 = F$ не делятся на 3. Поэтому по китайской теореме об остатках для $a,b\in\mathbf{Z}$ с условиями $3a\equiv 1(\mathrm{mod}\,F)$, $Fb\equiv 1(\mathrm{mod}\,3)$ выполняется соотношение

$$2N\cdot Z(k)\equiv 3az(k)\cdot 2N + Fbz_2(k)\cdot 2N\left(\mathrm{mod}\,F_N^2\right),$$

откуда следует, что справедливо сравнение

$$Z(k)\cdot 2N\equiv z(k)\cdot 2N(\mathrm{mod}\,F),$$

причем элемент $2N$ обратим в кольце $\mathbf{Z}/F\mathbf{Z}$. Отсюда следует, что $Z(k)\equiv z(k)(\mathrm{mod}\,F)$, то есть истинное значение $z(k)$ свертки получается редуцированием $Z(k)$ по $(\mathrm{mod}\,F)$.

В таблице 3.6 указаны некоторые "короткие" длины M-точечной свертки, для которых возможно параллельное вычисление, свободное от умножений.

Таблица 3.6

Допустимые модули для параллельного вычисления свертки длины $M\ (4 \le M \le 64)$

M	**Модули**	***M***	**Модули**
4	f_1	23	$q_{23}; M_{23}^1, M_{23}^7, M_{23}^2$
5	$q_5; M_5^7, M_5^2$	26	$F_{13}^1, M_{26}^1, F_{13}^7, F_{13}^2$
6	F_3^1, F_3^7	28	F_{14}^1, F_{14}^7
7	$q_7; M_7^1, M_7^7, M_7^2$	29	$q_{29}; M_{29}^1, M_{29}^7, M_{29}^2$
8	f_2	31	$q_{31}; M_{31}^1, M_{31}^7, M_{31}^2$
9	M_9^1, M_9^7	32	$f_4; F_{16}^7$
10	F_5^7, F_5^2	34	$F_{17}^1, M_{34}^1, F_{17}^7$
11	$q_{11}; M_{11}^1, M_{11}^2$	37	$q_{37}; M_{37}^1$
12	F_6^1, F_6^7	38	$F_{19}^1, F_{19}^7, F_{19}^2$
12	F_6^1, F_6^7	41	q_{41}
13	$q_{13}; M_{13}^1, M_{13}^7, M_{13}^2$	43	q_{43}
14	F_7^1, F_7^7, F_7^2	44	F_{22}^7
16	$f_3; F_8^1, F_8^7$	46	$F_{23}^1, F_{23}^7, F_{23}^2$
17	$q_{17}; M_{17}^1, M_{17}^7$	47	q_{47}
18	F_9^1	53	q_{53}
19	$q_{19}; M_{19}^1, M_{19}^2$	58	$F_{29}^1, F_{29}^7, F_{29}^2$
20	F_{10}^1, F_{10}^7	62	$F_{31}^1, F_{31}^7, F_{31}^2$
22	$F_{11}^1, F_{11}^7, F_{11}^2$	64	$f_5; F_{32}^1$

Приняты обозначения:

q_k - число Мерсенна: $q_k = 2^k - 1$; $f_k = 2^{2^k} + 1$ - число Ферма: $f_k = 2^{2^k} + 1$; M_n^1 и F_n^1 есть $\mathbf{Z}(i)$ - числа Мерсенна и Ферма соответственно; M_n^7 и F_n^7 – $\mathbf{S}\left(i\sqrt{7}\right)$ – числа Мерсенна и Ферма соответственно; M_n^2 и F_n^2 – $\mathbf{S}\left(i\sqrt{2}\right)$ – числа Мерсенна и Ферма соответственно.

3.4. Параллельные алгоритмы вычисления свертки в канонических системах счисления для расширений высоких степеней

Описание предложенной выше методики параллельного вычисления дискретной свертки было бы неполным, если бы мы не попытались увязать ее с существованием (канонических систем) счисления в кольцах целых элементов полей алгебраических чисел степени над $\mathbf{Q}$ выше второй. Пример экстраполяции такой методики на поля третьей степени рассмотрен выше во второй части пособия на примере чисел Ферма.

Более точно рассматривалось кольцо $\mathbf{S}$ целых элементов поля $\mathbf{F}$ разложения полинома $\varphi(z) = z^3 + 2$ над $\mathbf{Q}$. В кольце $\mathbf{S} \supset \mathbf{Z}$ для числа f наряду с обычным представлением составного числа в виде произведения целых рациональных чисел возможно представление в форме

$$f = \left(2^t \sqrt[3]{2} + 1\right)\left(2^t \gamma \sqrt[3]{2} + 1\right)\left(2^t \overline{\gamma} \sqrt[3]{2} + 1\right),$$

где γ - примитивный корень третьей степени из единицы. Возможность применения китайской теоремы об остатках гарантировалось леммой, утверждавшей, что элементы

$f_1 = \left(2^t \sqrt[3]{2} + 1\right)$, $f_2 = \left(2^t \gamma \sqrt[3]{2} + 1\right)$, $f_3 = \left(2^t \overline{\gamma} \sqrt[3]{2} + 1\right)$

попарно взаимно просты в кольце $\mathbf{S}$.

"Покомпонентные" вычисления в фактор-кольцах $\mathbf{S}/\mathbf{p}$, $\mathbf{S}/\mathbf{q}$, $\mathbf{S}/\mathbf{r}$, где $\mathbf{p} = (f_1)$, $\mathbf{q} = (f_1)$, $\mathbf{r} = (f_1)$ - главные идеалы, порожденные элементами f_1, f_2, f_3, реализовывались в редуцированных системах счисления с основаниями

$\left(\sqrt[3]{2}\right)$, $\left(\gamma\sqrt[3]{2}\right)$, $\left(\overline{\gamma}\sqrt[3]{2}\right)$.

Пусть теперь $\mathbf{S}$ - кольцо целых элементов поля $\mathbf{F}$ разложения некоторого полинома $\Phi_{kj}(x)$ степени k над $\mathbf{Q}$; $\alpha_{kj}^{(\nu)}$ $(\nu = 1,\ldots,k)$ - его корни в поле $\mathbf{F}$.

Можно рассмотреть "фермаподобные" целые рациональные числа

$$F_n\left(\Phi_{kj}\right) = \prod_{\nu=1}^{n}\left(\left(\alpha_{kj}^{(\nu)}\right)^n + 1\right)$$

как элементы кольца $\mathbf{S}$ и "мерсенноподобные "целые рациональные числа

$$M_n\left(\Phi_{kj}\right) = \prod_{\nu=1}^{n}\left(\left(\alpha_{kj}^{(\nu)}\right)^n - 1\right)$$

как элементы того же кольца.

Дальнейшие этапы экстраполяции методов предыдущих разделов главы на поля разложения многочленов $\Phi_{kj}(x)$ требуют ответов на следующие вопросы.

1. В каких кольцах целых элементов полей, ассоциированных с многочленами $\Phi_{kj}(x)$, существуют обобщения канонических систем счисления?

2. Являются ли алгебраические числа $\left(\left(\alpha_{kj}^{(\nu)}\right)^n - 1\right)$ при $\nu = 1,\ldots,k$ *попарно взаимно простыми?*

3. Есть ли среди чисел $F_n\left(\Phi_{kj}\right)$ и $M_n\left(\Phi_{kj}\right)$ простые?

4. Существуют ли аналоги (псевдо)нормальных составных чисел $F_n\left(\Phi_{kj}\right)$ и$M_n\left(\Phi_{kj}\right)$?

Если ответ на первый вопрос для бинарных систем счисления недавно получен, то доказательство попарной взаимной простоты чисел $\left(\left(\alpha_{kj}^{(\nu)}\right)^n - 1\right)$ требует глубокого "ручного" анализа арифметических свойств этих полей с привлечением теории Галуа (ср. с доказательством Леммы 3.4, в которой рассматривается не самый сложный случай). Авторы оставляют такой анализ за рамками настоящего пособия.

Ответы на второй и третий вопрос могут быть получены в результате непосредственных вычислений.

В таблицах 3.8 – 3.11 приведены результаты таких вычислений.

Таблица 3.7

Многочлены $\Phi_{kj}(x)$, в полях разложения которых существуют бинарные канонические системы счисления

k	$\Phi_{kj}(x)$
$k=3$	$\Phi_{31}(x)=2+x+x^3$
	$\Phi_{32}(x)=2+x^3$
	$\Phi_{33}(x)=2+x+x^2+x^3$
	$\Phi_{34}(x)=2+2x+2x^2+x^3$
$k=4$	$\Phi_{41}(x)=2+x+x^4$
	$\Phi_{42}(x)=2+x^4$
	$\Phi_{43}(x)=2+x^2+x^4$
	$\Phi_{44}(x)=2+x^2+x^4$
	$\Phi_{45}(x)=2+2x^2+x^4$
	$\Phi_{46}(x)=2+x+x^3+x^4$
	$\Phi_{47}(x)=2+x+x^2+x^3+x^4$
	$\Phi_{48}(x)=2+2x+x^2+x^3+x^4$
	$\Phi_{49}(x)=2+x+2x^2+x^3+x^4$
	$\Phi_{4,10}(x)=2+2x+2x^2+x^3+x^4$
	$\Phi_{4,11}(x)=2+2x+2x^2+2x^3+x^4$
	$\Phi_{4,12}(x)=2+3x+3x^2+2x^3+x^4$
$k=5$	$\Phi_{51}(x)=2+x+x^5$
	$\Phi_{52}(x)=2+x^5$
	$\Phi_{53}(x)=2+x+x^2+x^5$
	$\Phi_{54}(x)=2+x^2+x^3+x^5$
	$\Phi_{55}(x)=2+x+x^4+x^5$
	$\Phi_{56}(x)=2+x+x^2+x^3+x^4+x^5$
	$\Phi_{57}(x)=2+2x+2x^2+2x^3+2x^4+x^5$

Таблица 3.8

Факторизация чисел $F_n(\Phi_{kj})$ и $M_n(\Phi_{kj})$ при $\Phi_{31}(x) = 2 - x + x^3$

N	**Факторизация** $F_n(\Phi_{kj})$	**Факторизация** $M_n(\Phi_{kj})$
1	-2	-2
2	2^3	2^2
3	-2	-2×13
4	4	2^5
5	-2×11	-2×31
6	$2^3$13	$2^2\times13$
7	-2×113	-2×29
8	2^2 113	2^7
9	-2×307	-2×13×19
10	$2^3$101	2^2 11×31
11	-2×617	-2×23×67
12	$2^2\times769$	$2^5\times13^2$
13	-2×53×79	-2× 3^3 157
14	2^3 2549	2^2 29×113
15	-2×11×31×61	-2×13× 31^2
16	2^2 97×193	2^9 113
17	-2×103×613	-2×69161
18	2^3 13×2161	2^2 13×307
19	-2× 226937	-2×300277
20	2^2 41×6121	2^5 11×31×101

Таблица 3.9

Факторизация чисел $F_n\left(\Phi_{kj}\right)$ и $M_n\left(\Phi_{kj}\right)$ при $\Phi_{32}(x) = 2 + x^3$

N	**Факторизация** $F_n\left(\Phi_{kj}\right)$	**Факторизация** $M_n\left(\Phi_{kj}\right)$
1	-1	-3
2	**5**	3
3	-1	-3^3
4	**17**	3×5
5	**-31**	-3×11
6	5^3	3^3
7	**-127**	-3×43
8	**257**	3×5×17
9	-7^3	-3^6
10	5^2 41	3×11×31
11	-23×89	-3×683
12	17^3	$3^3 5^3$
13	-8191	-3×2731
14	5×29×113	3×43×127
15	-31^3	$-3^3 11^3$
16	**65537**	3×5×257
17	**-131071**	-3×43691
18	$5^3 13^3$	3^6 7^3
19	**-524287**	-3×174763
20	17×61681	3×5^2 11×31×41

Таблица 3.10

Факторизация чисел $F_n(\Phi_{kj})$ и $M_n(\Phi_{kj})$ при $\Phi_{33}(x) = 2 + x + x^2 + x^3$

N	**Факторизация** $F_n(\Phi_{kj})$	**Факторизация** $M_n(\Phi_{kj})$
1	-1	-5
2	1	5
3	-2^2	$-2^2 \times 5$
4	**41**	5
5	**-41**	-5^2
6	$2^2 \times 13$	$2^4 \times 5$
7	**-71**	-5×43
8	**337**	5×41
9	$-2^2 163$	$-2^2 5 \times 19$
10	**1061**	$5^2 41$
11	-23×67	-5×23^2
12	$2^2\ 5^2 41$	$2^6 5 \times 13$
13	**-9283**	$-3^3 5 \times 53$
14	**17669**	5×43×71
15	$-2^2 41 \times 181$	$-2^2\ 5^2\ 19^2$
16	97×641	5×41×337
17	**-136273**	-5×25229
18	$2^2 13 \times 73^2$	$2^4 5 \times 19 \times 163$
19	-229×2243	-5×107123
20	$41^2 601$	$5^2 41 \times 1061$

Таблица 3.11

Факторизация чисел $F_n\left(\Phi_{kj}\right)$ и $M_n\left(\Phi_{kj}\right)$ при $\Phi_{34}(x) = 2 + 2x + 2x^2 + x^3$

N	**Факторизация** $F_n\left(\Phi_{kj}\right)$	**Факторизация** $M_n\left(\Phi_{kj}\right)$
1	-1	**-7**
2	1	**7**
3	**-13**	**-7**
4	**41**	**7**
5	**-11**	-7×11
6	**61**	7×13
7	**-239**	-7^2
8	289	7×41
9	-247	-3×7×19
10	**1361**	7×11^2
11	**-2927**	-7×199
12	41×73	7×13×61
13	-53×131	$-3^3\,7\times53$
14	29×757	$7^2\,239$
15	-11×13×241	-7×11×421
16	**50177**	$7\times17^2\,41$
17	**-140863**	-7×17783
18	61×5077	7×13×19×127
19	**-470783**	-7×83639
20	41×23321	$7\times11^2\,1361$

ПРИМЕЧАНИЯ

Модулярные версии дискретного преобразования Фурье (теоретико-числовые преобразования (ТЧП), преобразования Фурье-Галуа) были введены практически одновременно в работах Р.Г.Фараджиева и Я.З.Ципкина [14],[15], А.Штрассена и В.Шёнхаге [16], а затем фактически переоткрыты в работе Ч.Рейдера [17], [18]. Работа [17] получила наибольшую известность и ее результаты многократно обобщались. Пик популярности ТЧП приходится на 70-е годы. Возрождение интереса к этой проблематике связано с разработкой СБИС нового поколения [20]- [23], а также необходимостью быстро и точно производить умножения больших целых чисел, в первую очередь, при решении задач криптографии.

С "классикой" теории ТЧП можно ознакомиться в [11], [12], [19], [24]. Русские переводы основополагающих статей по ТЧП содержатся в [25]. Хороший обзор результатов до 1996г. приведен в [21]. Со свойствами чисел Голомба, Мерсенна и Ферма в контексте рассматриваемых задач можно ознакомиться в [24], а с основными фактами из теории p-адических чисел - по учебнику [6].

Идея рассмотрения "комплексных" преобразований Мерсенна принадлежит Рейдеру (см. [25]). Первые упоминания о p-адических числах при вычислении свертки встречается, по-видимому, в статьях [27] и [28]. Метрическая интерпретация идеи параллельного использования комплексного и модулярного ДПФ для вычисления свертки опубликована автором в [29], хотя идея уточнения результатов вещественных/комплексных вычислений с помощью модулярных неявно используется, например, в [26].

Экстраполяция метода и результатов на случай модулей p более общего вида $p = b^k \pm 1$ также не вызывает принципиальных затруд-

нений. В [34] приведены разложения чисел p указанного вида на простые множители. Практическая целесообразность такого обобщения ограничивается исключительно возможностями вычислительных средств, ориентированных на недвоичное представление информации.

Авторы не нашли работ других авторов, прямо использующих альтернативные разложения колец по модулям составных чисел Мерсенна и Ферма в прямую сумму подколец специального вида, ассоциированного с "удобной" системой счисления. В какой-то степени идейным предшественникоми можно считать работу [35].

СПИСОК ЛИТЕРАТУРЫ

1. Рабинер Р., Гоулд Б. *Теория и применение цифровой обработки сигналов*. М.:Мир, 1978.

2. *Методы компьютерной обработки изображений* / Под ред. В.А.Сойфера. М.:Наука., 2001,

3. Кнут Д. *Искусство программирования для ЭВМ*. Т. 2. – М.: Мир, 1977

4. Колмогоров А.Н., Фомин С.В. *Элементы теории функций и функционального анализа*. М.:Наука, 1976.

5. Рудин У. *Основы математического анализа*. М.:Мир, 1966.

6. Боревич З.И., Шафаревич И.Р. *Теория чисел*. М.:Наука, 1972

7. Ван дер Варден Б.Л. *Алгебра*. М.: Наука, 1976.

8. Айерленд К., Роузен М. *Классическое введение в современную теорию чисел*. М.:Мир, 1987.

9. Эдвардс Г. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел.* М.: Мир, 1980.

10. Виноградов И.М. *Основы теории чисел*. М.:Наука, 1965.

11. Блейхут Р. *Быстрые алгоритмы цифровой обработки сигналов*. М.: Мир, 1989.

12. Нуссбаумер Г. *Быстрое преобразование Фурье и алгоритмы вычисления сверток*. М.: Радио и связь, 1985.

13. Торгашев В.А. *Система остаточных классов и надежность ЦВМ*. М.: Сов. радио, 1973.

14. Фараджиев Р.Г. Аналитические способы вычисления процессов в линейных последовательных машинах // *Изв. АН СССР. Техн. Киберн.*, 1965. N 5. – С. 74-80.

15. Фараджиев Р.Г., Ципкин Я.З. Преобразование Лапласа-Галуа в теории последовательных машин. *ДАН СССР*. Т. 166, 1966. N 36. С. 45-52.

16. Schoenhage A., Strassen V. Schnelle Multiplikation grosser Zahlen. *Computing.* 1966. B.7, N.3/4. – P. 281-292.

17. Rader C.M. Discrete convolution via Mersenne transorm // *IEEE Trans. Comp*, 1972. C-21. – P.1269-1273.

18. Rader C.M. On the application of the number theoretic methods of high-speed convolution to two-dimensional filtering // *IEEE Trans. on Circuits and Systems*, 1975. V.22. – P.575.

19. Ноден П., Китте К. *Алгебраическая алгоритмика.* М.: Мир, 1999

20. Alfredson L.-I. A fast Fermat number transform for long sequences // *Proc. EUSIPCO-94*, Edinburg, Scotland, 1994. V.111. – P.1579-1581.

21. Alfredson L.-I.. VLSI architectures and arithmetic operations with application to the Fermat number transform // *Linkőoping Studies in Sci. and Technology*, Dissertation No.425, 1996.

22. Boussakta S., Holt A.G.J. Calculation of the discrete Hartley transform via Fermat number transform using VLSI chip // *IEE Proc.*, 1988. V. 135, Pt.G, N 3. – P.101-103.

23. Towers P.J., Pajayakrit A., Holt A.G.J. Cascadable NMOS VLSI circuit for implementing a fast convolver using the Fermat number transform // *IEE Proc.*, 1987. V.135, Pt.G, 2. – P.57-66.

24. Вариченко Л.В., Лабунец В.Г., Раков М.А. *Абстрактные алгебраические системы и цифровая обработка сигналов.* Киев: Наукова думка, 1986.

25. Маккеллан Дж.Х., Рейдер Ч.М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983.

26. Дэвенпорт Дж., Сирэ И., Турнье Э. *Компьютерная алгебра*. М.: Мир, 1991.

27. Skula L. Linear transforms and convolution // *Math. Slovaca*, 1987. v.37. No 1. – pp.9-30.

28. Soo-Chang Pei. Exact fast digital convolution by using *p*-adic numbers and polynomial transformations // *IEEE Trans. ICASSP 85,* 1985. V.2. – P. 760-763.

29. Чернов В.М. О точности вычисления дискретной круговой свёртки в нормированных полях // *Автоматика и вычислительная техника*, 1992. № 1. – С. 53-57.

30. Боревич З.И., Шафаревич И.Р. *Теория чисел*. М.: Наука, 1985.

31. Хассе Х. *Лекции по теории чисел*. М.: ИЛ, 1953.

32. Постников М.М. *Теория Галуа*. М.: Наука, 1962.

33. Ленг С. *Алгебра*. М.: Мир, 1965.

34. Brillart J., Lehmer D.H., Selfridge J.L., Tuckerman B., Wagstaff S.S. *Factorization of* $b^n \pm 1$, *b=2,3,5,6,7,10,11,12 up high powers //* Contemp.Math.-AMS, 1988. V.22.

35. Лабунец В.Г. Теоретико-числовые преобразования над полями алгебраических чисел, *Применение ортогональных методов при обработке сигналов и анализе систем*. Свердловск: УПИ, 1981. – С.44-53.

36. Чернов В.М. Факторизация целых элементов полей алгебраических чисел и быстрые алгоритмы теоретико-числовых преобразований // *Тез. докл. 8-й Всерос. конф. "Математические методы распознавания образов"*. М.: 1997. – С.121.

37. Чернов В.М. Синтез параллельных алгоритмов преобразований Фурье-Галуа в прямых суммах конечных колец // *Известия Самарского научного центра Российской Академии Наук*, 2000. №2, Вып.1. – С.128-133.

38. Chernov V.M., Pershina M.V. Error-free" calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields. // G.Sommer, K.Daniilidis, J.Pauli (Eds) "*Computer Analysis of Image and Pattern*". (CAIP'97). Springer Verlag. (Lecture Note Computer Science) 1296. – P.621-628.

39. Gilbert W.J., Complex numbers with three radix expansions // *Canad. J. Math.,* 1982. V.34. – P.1335-1348.

40. Gilbert W.J., Arithmetic in complex bases // *Math. Mag.,* 1984. V.57. – P.77-81.

41. Matula D.W. Basic digit sets for radix representation // *J. Assoc. Comput. Mach.*, 1982. V.29. – P.1131-1143.

42. Odlyzko A.M. Non-negative Digit Sets in Positional Number Systems // *Proc. London Math. Soc.*, 1978. V.37. – P.213-229.

43. Sylvester J.J. Note on Complex Integers (by Lanavicensis) // *Quart. J. Pure and Applied Math.*, 1861. V.4. – P.94-96; 124-130.

44. Kátai I., Kovács B. Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen // *Acta Sci. Math. (Szeged),* 1980. B.42. – P.99-107.

45. Kátai I., Kovács B. Canonical Number Systems in Imaginary Quadratic Fields // *Acta Math. Acad. Sci. Hungaricae*, 1981. V.37. – P.159-164.

46. Kátai I., Szabó J. Canonical number systems for complex integers // *Acta Sci. Math. (Szeged),* 1975. V.37. – P. 255-260

47. Davio M, Deschamps J.P., Gossart C. *Complex arithmetic*, Philips M.B.L.E. Research Lab. Report, R369, May 1978, Brussels.

48. Gauss C.F., *Werke I.I.* Königlichen Gesellschaft der Wissenschaften, Göttingen, 1863. (Reprinted by Georg Olms, Hildesheim, 1973).

49. Gilbert W.J. Radix representations of quadratic fields // *J. Math. Anal. Appl*, 1981. V.83. – P. 264-274.

50. Gilbert W.J. Fractal Geometry derived from Complex Bases // *Math. Intelligencer*, 1982. V.4. – P. 78-86.

51. Gilbert W.J. The Fractal Dimension of Sets derived from Complex Bases // *Canad. Math. Bull.*, 1986. V.29. – P. 495-500.

52. Kovács B. Pethö A. Number systems in integral domains, especially in orders of algebraic number fields // *Acta Sci. Math. (Szeged),* 1991. V. 55. – P. 287-299.

53. Thuswaldner J.M. Elementary Properties of Canonical Number Systems in Quadratic Fields // *Applications of Fibonacci Numbers* , F.T.Howard (Editor), 1998. V.7, Kluwer. – P.405-409.

54. Kovacs A. Generalized binary number systems. Annales Univ. Sci. Budapest, Sect. Comp.20, 2001. – P. 195-206.

55. Akiyama S., Petho A. On Canonical Number Systems // Theoret. Comp. Sci., 2002. V. 270. – P. 921-933.

56. Brunotte H. On trinomial basis of Radix Representations of Algebraic Integers // Acta Sci. Math. (Szeged), 2001. V.67 – P. 407-413.

57. Kovacs B. Canonical number systems in algebraic number fields // Acta Math. Acad. Sci. Hungar, 1981. V.37. – P. 405-407.

58. Petho A. On a polynomial transformation and its application to the construction of a public key cryptosystem. Computational Number Theory, Proc, Walter de Gruyter Publ. Comp. Eds.: A. Petho, M. Pohst, H.G. Zimmer and H.C. Williams. 1991. – P. 31-44.

59. Scheicher, Kanonische Ziffernsysteme und Automaten, Grazer Math. Ber., 333 (1997), 1-17.

60. Allouche J.-P., Cateland E., Gilbert W.J., Peitgen H.-O., Shallit I., and G. Skordev. Automatic maps in exotic numeration systems. Theory Com-put. Syst. (Math. Systems Theory), 30:285-331, 1997.

61. Frougny C. and Solomyak B.. On representation of integers in linear numeration systems // Ergodic Theory of $\square^d$ actions, Proceedings of the Warwick Symposium, Warwick, UK, 1993-94, Eds. M. Pollicott et al. Cambridge University Press, Lond. Math. Soc. Lect. Note Ser., 228:345-368, 1996.

62. Kovacs B. CNS rings, in: Topics in Classical Number Theory, vol. II, Colloq. Math. Soc. Jdnos Bolyai, Ed. G. Haldsz, North Holland, 34:961 971, 1984.

63. Kormendi S. Canonical number systems in $Q(\sqrt[3]{2})$, Acta Sci. Math. (Szeged) 50, 351 – 357, 1986.

64. Kovacs A. On number expansion in lattices // Proc. 5th International Conference on Applied Informatics, Eger, Hungary, 2001, submitted to Comp. Math. Appl.

65. Daroczy Z., Katai I. Generalized number systems in the complex plane // Acta Sci. Math. Hung. 51 (3-4) (1975) 409-416.

66. Duprat J., Herreros Y., Kla S., New redundant representations of complex numbers and vectors // IEEE Trans. Comput., 1993. V.42 (7). – P. 817-824.

67. Safer T. Radix representations of algebraic number fields and finite automata // Proc. STACS '98, to appear.

68. Vince A. Replicating tesselations, SIAM J. Discrete Math. 6, 1993. – P.501-521.

69. Steidl G. On symmetric representation of Gaussian integers, BIT 29, 1989. – P.563-571.

70. G. Farkas, Number systems in real quadratic fields, Annales Univ. Sci. Bud. Sect. Comp. 18, 47-59, (1999).

71. Farkas G. Digital expansions in real algebraic quadratic fields // Math. Pannonica 10 (2), 1999. – P. 235-248.

72. Katai I. Construction of number systems in algebraic number fields. Annales Univ. Sci. Bud. Sect. Comp. 18, 103-107, (1999).

73. Grossman E.H. Number bases in quadratic fields. Studio Sci. Math. Hungar, 1985. V. 20. – P. 55-58.

Учебное издание

Чернов Владимир Михайлович,
Корепанов Андрей Олегович,

ТЕОРЕТИКО-ЧИСЛОВЫЕ ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Учебное пособие

Технический редактор *В.В. Сергеев*
Редакторская обработка *Н.В. Прядильникова*
Корректорская обработка *И.И. Проломова*
Доверстка *О.Ю. Дьяченко*

Подписано в печать 28.12.06. Формат 60х84 1/16.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 6,5. Усл. кр.-отт. 6,6. Печ.л. 7.
Тираж 50 экз. Заказ . ИП – 51/2006.

Самарский государственный
аэрокосмический университет.
443086 Самара, Московское шоссе, 34.

Изд-во Самарского государственного
аэрокосмического университета.
443086 Самара, Московское шоссе, 34.